PRISTINE LANDSCAPES
IN ELEMENTARY MATHEMATICS

PRISTINE LANDSCAPES IN ELEMENTARY MATHEMATICS

Titu Andreescu

Cristinel Mortici

Marian Tetiva

Library of Congress Control Number: 2016917207

ISBN-10: 0-9968745-7-7
ISBN-13: 978-0-9968745-7-1

© 2016 XYZ Press, LLC

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (XYZ Press, LLC, 3425 Neiman Rd., Plano, TX 75025, USA) and the authors except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden. The use in this publication of tradenames, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

9 8 7 6 5 4 3 2 1

www.awesomemath.org

The cover image is an *iSock* photo.

Cover design by Iury Ulzutuev

Preface

This book is about taking familiar ideas (and perhaps some not-so-familiar ones!) and extending them to solve a broad variety of problems. The intended audience is the ambitious high school or college student who is seeking a substantive "big picture" view of several topics that often present themselves at the Olympiad level of mathematics competitions or in proofs and applications of classical results. This "big picture" view of a topic suggests the metaphor of a *landscape.* Landscapes are rich in detail and often contain subtleties that are embedded for the discerning eye to discover.

And so are the chapters and problems that follow. As we shall soon see, sometimes the simplest of ideas can hold very powerful abstractions, or can be used to solve a wide range of problems. It is our hope that this book will offer the reader an ample variety of both breadth and depth in its subject matter. The topics covered span the broad subject areas of algebra, geometry, number theory, and even a few elements of mathematical analysis while each chapter explores specific themes and ideas that illustrate the aforementioned subject areas.

Each chapter is composed of three parts: the theoretical discussion, proposed problems, and solutions to the proposed problems. In each chapter, the theoretical discussion sets the stage for a different landscape by introducing and motivating the themes of that chapter — often with a review of some definitions or classical results. The remainder of the theoretical part of each chapter is devoted to examining illustrative examples — that is, several problems are presented, each followed by at least one solution. It is assumed that the reader is intimately familiar with topics covered in the standard high school mathematics curriculum up through and including precalculus. For some chapters, it will be helpful for the reader to have had previous exposure to topics from discrete mathematics and number theory.

As you experience these "landscapes" in each chapter, the reader is encouraged to carefully seek out the finer points and subtleties. To summarize: *don't rush.* These landscapes provide a "view" into areas that are not typically encountered in great depth in standard coursework, but nonetheless have profound implications. It is also our hope that even if the reader happens not to be well-versed in proofs, he or she will appreciate and grasp the level of *rigor* and thinking that is required in formulating logical and convincing arguments. We hope the examples and the suggested solutions to the problems lend insight not only to the underlying mathematics, but also serve as examples of good mathematical exposition.

We want to express our thanks to our friends Gabriel Dospinescu and Chris Jeuell for their great help throughout our work to the manuscript; they surely had a big contribution to improving it and giving it a better final form.

We invite you to enjoy and appreciate our selection of these beautiful landscapes that abound in mathematics.

Titu Andreescu, Cristinel Mortici, Marian Tetiva

Contents

Preface v

1 The Ubiquitous Pigeonhole Principle 1

2 A Property of the Greatest Common Divisor 23

3 Squares 51

4 Digital Sums 75

5 Arithmetic and Geometric Progressions 97

6 Complementary Sequences 113

7 Quadratic Functions and Quadratic Equations 129

8 Parametric Solutions for Certain Equations 145

9 The Scalar Product 161

10 Equilateral Triangles in the Complex Plane 179

11 Recurrence Relations 197

12 Sequences Given by Implicit Relations 217

13 Matrices Associated to Second Order Recurrences 235

14 Final Problem Set 255

Bibliography 277

Other Books from XYZ Press 279

Chapter 1

The Ubiquitous Pigeonhole Principle

Oh, no, not again! — we hear you say, and you might be right — or you might not. The pigeonhole principle appears in numerous books and magazines and places on the Internet, and everyone is familiar with it, and everybody knows what is "all" about this principle with a bizarre name that.... Who needs another lesson on it? Well, this point of view may be valid — or it may be not. Just read and smile (since we start with the simplest examples), then enjoy (because we will move on to harder problems). Constantin Noica, a great Romanian philosopher, used to say that you can begin to learn philosophy from anywhere — start with any book you want, with any philosopher that you please. Apparently this doesn't work very well for mathematical training, but we say that a good point to start in mathematics is the *pigeonhole principle.* As humble as it may seem, the pigeonhole principle is an indispensable tool throughout all of mathematics. As said in the chapter title, you can find it anywhere in this beautiful realm of human knowledge to which we (and our readers) dedicated our lives, thus we decided to offer the opening chapter of our book to this marvelous (by its simplicity) idea. Last, but not least, remember that another name for the pigeonhole principle is *Dirichlet's drawer principle* (it seems that he was the first to use it explicitly); if it is related to such a great mathematician's name as Dirichlet, it must be worth studying, right?

We are sure that the reader is acquainted with the spectacularly simple statement of the pigeonhole principle (or, if he/she is not, let him/her be from now on). It says that if you try to put in a few boxes a few objects, the number of which exceeds the number of boxes, then, necessarily, there is (at least) one box that contains more than one object. (If you put five pigeons in four pigeonholes, two or more pigeons need to jostle each other into the same pigeonhole.) To put it more formally, we have:

The pigeonhole principle/Dirichlet's drawer principle. If we want to distribute $m > n$ objects into n boxes, then there will exist (at least) one box that contains (at least) two objects.

If we want to push this formalism further, we can state it as follows:

The pigeonhole principle/Dirichlet's drawer principle. If A and B are finite sets with $|A| > |B|$ (the number of elements of A is greater than the number of elements of B), then there is no injective function from A to B.

(Consider A as the set of pigeons and consider B as the set of pigeonholes; a function from A to B puts pigeons in the pigeonholes, and there must be more than one pigeon in some pigeonhole, thus the function cannot be injective.) Actually, this form won't be necessary for our tasks, but it might be interesting for further developments.

For instance, if you have a pile of red and blue balls, you have to take (at least) three of them in order to be sure that you get two balls of the same color. In this example the pigeonholes are the colors (red and blue) and their number is, of course, 2 — so you need have three or more pigeons (balls) to be sure that at least two of them fall into the same box (that is, they have the same color). Or, because everyone of us has on his or her head at most (say) a million hairs, you can gather together arbitrarily 1000001 people and bet them that there are two of them with the same number of hairs on their heads. Bet on one dollar to each of them that your guess is true and you will surely win, won't you? And you will be a millionaire only by properly applying the pigeonhole principle. (Of course, it will be hard to count all the hairs in their heads, so you can think of something more practical, like: gather together q people and bet with them that there exist among them two with the same birthday. What value of q should be chosen to assure winning? We are sure you already know. And don't be sad about losing a million: there will be less money, but this win is accomplishable and it is easy money, isn't it?) Let us move on now to "serious" problems.

Problem. From any n people we can always choose two with the same number of acquaintances among the others $n - 1$.

Solution. If $n = 1$, this is vacuously true, while if $n = 2$, the two persons can be acquainted to each other, or not: in both cases they have the same number of acquaintances among the other(s). (Of course we consider "acquaintanceship" to be a symmetric relation, as will it be in all such problems: A knows B if and only if B knows A. Also, we don't consider that A knows A — the relation is not reflexive.) If there are three people each of whom knows each other (or each of whom does not know each other) the conclusion is plain. Two cases remain: when two persons (say A and B) know the third (name it C) but don't know each other, and when A and B are acquainted, but neither of them is acquainted to C. In both cases A and B have the same number of acquaintances among the others.

However, this is clearly *not* a path to follow for solving this problem: things get more and more complicated when n increases. On the other hand, the pigeonhole principle solves it (almost) immediately. Namely, each of the n persons can have at most $n - 1$ acquaintances among the others. There are n persons (pigeons) and only $n - 1$ possibilities for the number of the acquaintances (pigeonholes), so there must be two persons with the same number of acquaintances. Done... or not?

Of course, we forgot that the number of persons that someone knows among the others could also be 0: we didn't say that there isn't a person knowing none of the others, so the above solution works *only* in the case when everybody knows at least one person in the group. However, this flaw is not hard to fix. If there are *at least two* such persons, the problem is clearly solved. Otherwise, each and every one of the other $n - 1$ has a number of acquaintances from 1 to $n-2$ (that is, at most $n-1$ known people), and the above reasoning shows that there are two of them who know the same number of people among the others.

Solution. After analyzing the above facts, one can come with the following alternative (and much more simple) wording for solving the problem. Choose from the n people those k who know nobody in the entire group. Each of the $n-k$ remaining persons has at least one and at most $n-k-1$ acquaintances among the others, and the pigeonhole principle ensures us that there are two of them with the same number of acquaintances in the group. Simple, isn't? Actually, we see that the first case (when everybody knows at least somebody else) suffices to solve the problem anyway — the problem that can also be rephrased in terms of graph theory: in a (simple, undirected) graph on n vertices, there are always two vertices with the same degree (that is, two vertices from which the same number of edges come out).

Another well-known problem about people who know (or don't know) people is the following.

Problem. Prove that in any group of six people there are three who know each other, or there are three who don't know each other (mutually).

Solution. It is easier to speak if we use the language of graphs. Namely, let the six persons be represented by six points in the plane (the vertices of the graph) and draw a red (blue) line between two points if the persons represented by that line know each other (respectively if they do not know each other). We get the complete graph on 6 vertices with all edges (How many? It is not important for this problem, but think about it!) colored red or blue, and we want to prove that (for any such coloring) there exists either a red triangle, or a blue one. Of course, by a "red/blue triangle" we mean a triangle with all its edges colored red/blue. In order to solve this problem, we need the following more general, often used, form of the principle:

General pigeonhole principle. If more than nk objects are to be placed in n boxes, then there exists (at least) one box containing (at least) $k+1$ objects.

(For if each of the n boxes contained at most k objects, there would be at most nk objects, which is not the case. For $k=1$ we get the principle as stated above.) Now let us go back to our problem. Look at one (arbitrarily chosen) vertex A and the five edges incident with it. Because $5 = 2 \cdot 2 + 1$ and there are only two colors (the boxes, or the pigeonholes) there must be three edges from that vertex that have all the same color. Name those edges AB, AC, and AD, and suppose (without loss of generality) that their common color is red. We are now almost done. Indeed, if one of the edges BC, BD, and CD is red, we have a red a triangle: ABC, or ABD, or ACD. Otherwise BC, BD, and CD are all blue, and the triangle BCD is blue.

Note also that the general form of the principle can be extended to the following one, referring to infinitely many objects:

The pigeonhole principle — the infinite case. Consider infinitely many objects to be placed into n (thus finitely many) boxes. Then there exists a box that contains infinitely many objects.

We use this version to prove the following theorem of Schur.

Theorem. *Let the set of positive integers be partitioned into finitely many classes. Then there exist three numbers x, y, and z in the same class of the partition such that $x+y=z$ (x and y need not necessarily be distinct).*

Proof. Let us consider that $\mathbb{N}^*$ is partitioned into three classes A, B, and C, and let $a_1 < a_2 < \cdots$ be the elements of A (of course, at least one of A, B, and C must be infinite, and we can assume, without loss of generality, that A is infinite). If any of the positive integers $a_2 - a_1, a_3 - a_1, \ldots$ belongs to A, we are done (if, say, $a_i - a_1 = a_j$, we also have $a_1 + a_j = a_i$, hence a solution for $x+y=z$ with all x, y, and z belonging to A). Otherwise, since any positive integer belongs to one (and only) of A, B, and C, one of the sets B and C contains infinitely many of the above differences (by the infinite case of the pigeonhole principle). Suppose (again without loss of generality) that the numbers $b_1 = a_{i_1} - a_1$, $b_2 = a_{i_2} - a_1, \ldots$ belong to B. If any of the differences $b_2 - b_1$, $b_3 - b_1, \ldots$ belongs to B, we clearly finished our proof (we get $x, y, z \in B$ such that $x+y=z$). Yet, if any of these numbers belongs to A, we have also completed our proof; indeed, if $b_m - b_1 = a_{i_m} - a_{i_1}$ belongs to A, this yields a solution to $x+y=z$ with all components in A. Now if $c_1 = b_2 - b_1$, $c_2 = b_3 - b_1, \ldots$ all belong to C, the differences $c_n - c_1 = b_{n+1} - b_2 = a_{i_{n+1}} - a_{i_2}$ have to be in one (and only one) of the sets A, B, and C, but (due to the threefold aspect of these differences) in any case a solution to $x+y=z$ appears in one of the three classes of the partition.

The reader is invited to write the proof in the general case, with an arbitrary (but finite) number of classes. Note that, actually, this is just a weak form of Schur's theorem, whose statement is as follows:

Theorem. *For every positive integer k, there exists a positive integer $S = S(k)$ such that, for any $N \geq S$, and for every k-class partition of $\{1, 2, \ldots, N\}$, one of the classes of the partition contains three numbers x, y and z such that $x + y = z$.*

The numbers $S(k)$ are named Schur's numbers, and their only known values are $S(1) = 2$, $S(2) = 5$, $S(3) = 14$, and $S(4) = 45$. The reader can try to prove that these values are correct, however we will move to other topics, since these problems are beyond the scope of this book.

Everybody knows that from any n integers, one can choose a few (at least one) whose sum is divisible by n. It is a classic result using Dirichlet's drawer principle. The other important idea for solving this problem is that two integers leave the same remainder when divided by n if and only if their difference is divisible by n. Based on the same ideas, one can prove the following result.

Problem. For any three integers a, b, and c, the number

$$N = abc(a - b)(a - c)(b - c)$$

is divisible by 3.

Solution. If any of the three numbers is divisible by 3, clearly N has the same property, too. Otherwise, a, b, and c give, when divided by 3, one of the remainders 1 or 2. So, we have three numbers (pigeons) that must fall into two residue classes modulo 3 (only 2 pigeonholes). The principle says that there exist two of the numbers in the same residue class — and then their difference is divisible by 3, therefore N (which has all three differences as factors) is divisible by 3, too. The reader can immediately generalize this to n numbers: if $a_1, \ldots, a_n$ are integers, then

$$N = a_1 \cdots a_n \prod_{1 \leq i < j \leq n} (a_i - a_j)$$

is divisible by n. Of course, this is not a very powerful statement (as long as one knows that $\prod_{1 \leq i < j \leq n} (a_i - a_j)$ is always divisible by $\prod_{1 \leq i < j \leq n} (i - j)$), but it is a good exercise for practicing (as a beginner) with the pigeonhole principle. Or, the reader may wish to prove that for all integers a, b, and c, the number

$$abc(a - 1)(b - 1)(c - 1)(a - b)(a - c)(b - c)$$

is divisible by 4.

Here are a few problems involving divisibility.

Problem. If $n + 1$ numbers are arbitrarily chosen from the set $\{1, 2, \ldots, 2n\}$, prove that there exist two among them that are relatively prime.

Solution. The pigeonholes are the sets $\{1,2\},\{3,4\},\ldots,\{2n-1,2n\}$, and the pigeons are our $n+1$ given numbers. Two pigeons must fall into the same pigeonhole, that is, two numbers are consecutive, therefore they are also relatively prime. Simple, isn't it? However read the following story before you decide that (if you didn't try to solve the problem first).

It seems that Erdős gave this problem (and others) to the twelve year old boy Louis Pósa, when he first met him, and they were having lunch. As Erdős himself (cited by Ross Honsberger) related, Pósa solved the problems before finishing his soup — and solved this particular problem in less than one minute. Which, by the way, Erdős didn't do at his time: he needed about ten minutes to find the above (simple and natural) solution.

Also note that n is the maximum number of numbers from $\{1,2,\ldots,2n\}$ such that any two share a common factor greater than 1, for we can choose $2,4,\ldots,2n$ (the even numbers) that have this property (actually they all share the same common factor, but this is not important for our problem).

Problem. Find the maximum number of numbers from $\{1,2,\ldots,2n\}$ such that no number divides another.

Solution. We can find n numbers with this property, namely $n+1$, $n+2,\ldots,2n$: no number divides another because the smallest multiple of the smallest number exceeds the greatest number. It remains to show that if we choose $n+1$ numbers from $\{1,2,\ldots,2n\}$, then there are two (distinct, of course) such that one divides the other. In order to do that, let's note that any positive integer x can be written in a unique manner as $x=2^y(2z+1)$ with nonnegative integers y and z. Although 2^y could also be odd (when $y=0$) we will call $2z+1$ the odd part of x thus expressed. Now our $n+1$ numbers have their odd parts at most equal to $2n-1$ (because they themselves are at most equal to $2n$), hence there are at most n possible odd parts for $n+1$ numbers. The conclusion according to the pigeonhole principle is that there must be two of the numbers that have equal odd parts — of course, in this case, the smaller number is a divisor of the larger number. Observe that a similar (basically identical) problem can be formulated with the set $\{1,2,\ldots,2n-1\}$ instead of $\{1,2,\ldots,2n\}$.

Problem. Let $m \geq 2$ and a be relatively prime integers. Prove that there are positive integers x and y, both less than or equal to $\sqrt{m}$, and such that one of $ax \pm y$ is divisible by m.

Solution. We consider all expressions $au+v$, with u and v running through the set $\{0,1,\ldots,[\sqrt{m}]\}$ (the square brackets indicate the integer part). Their number is $([\sqrt{m}]+1)^2 > (\sqrt{m})^2 = m$, therefore two of them have to yield the same remainder when divided by m. But if we have $au_1+v_1 \equiv au_2+v_2 \pmod{m}$ (with either $u_1 \neq u_2$, or $v_1 \neq v_2$), then $ax+y \equiv 0 \pmod{p}$ or $ax-y \equiv 0 \pmod{p}$, for $x=|u_1-u_2|$ and $y=|v_1-v_2|$. If we content ourselves with the fact that the requested x and y are nonnegative and not both zero, we can finish the proof here. But we need to show that x and y are strictly positive, so we continue. If $u_1 = u_2$, the above congruence leads to $v_1 \equiv v_2 \pmod{m}$, which, for v_1 and v_2 nonnegative and at most equal to $[\sqrt{m}]$ (thus less than or equal to $\sqrt{m}$) is possible only if we had $v_1 = v_2$. But in this case the pairs (u_1, v_1) and (u_2, v_2) would be equal, which is false. Yet, $v_1 = v_2$ implies $au_1 \equiv au_2 \pmod{m}$, therefore $u_1 \equiv u_2 \pmod{m}$ (because a is prime to m, hence invertible modulo m), then, as before, $u_1 = u_2$ and $(u_1, v_1) = (u_2, v_2)$, a contradiction. Thus $u_1 \neq u_2$ and $v_1 \neq v_2$, and x and y are strictly positive, as desired.

As simple as it may seem, this result (known as Thue's theorem) is important in proving great theorems. We give here only the example of Fermat's theorem about the representation of integers as sums of two squares (actually just one of the important steps for the proof of the general result).

Theorem. *Any prime $p \equiv 1 \pmod{4}$ can be expressed as the sum of two squares.*

Proof. By multiplying side by side all congruences $j \equiv -(p-j) \pmod{p}$, for $j = 1, 2, \ldots, (p-1)/2$, we get

$$1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \equiv (-1)^{(p-1)/2} \left(\frac{p+1}{2}\right) \left(\frac{p+3}{2}\right) \cdots (p-1) \pmod{p}.$$

But $p \equiv 1 \pmod{4}$ implies that $(p-1)/2$ is even, and if we multiply again this congruence by $((p-1)/2)!$, we get

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (p-1)! \pmod{p}.$$

Now, Wilson's theorem tells us that $(p-1)! \equiv -1 \pmod{p}$, thus we have

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}.$$

Or, we can say $a^2 + 1$ is divisible by p, for $a = ((p-1)/2)!$ — and we are done with the first step of the proof. In its classical variant, after obtaining a multiple of p that can be written as the sum of two squares, it is proven that the smallest such multiple is exactly p, thus getting the desired conclusion. However, with Thue's theorem at our disposal, we can go on like this. The number a with property that $a^2 + 1 \equiv 0 \pmod{p}$ is definitely relatively prime to p, hence, according to Thue's theorem, we can find positive integers x and y, each less than $\sqrt{p}$, such that either $ax - y \equiv 0 \pmod{p}$, or $ax + y \equiv 0 \pmod{p}$. In both cases we have $a^2x^2 - y^2 \equiv 0 \pmod{p}$. This congruence leads (by using $a^2 \equiv -1 \pmod{p}$) to $x^2 + y^2 \equiv 0 \pmod{p}$, that is, to the fact that $x^2 + y^2$ is a multiple of p. Yes, but we also have $x < \sqrt{p}$, and $y < \sqrt{p}$, hence

$x^2 + y^2 < p + p = 2p$. In conclusion, $x^2 + y^2$ is a nonzero multiple of p, which is also less than $2p$, so only the possibility $x^2 + y^2 = p$ remains, finishing the proof.

We end this section with a few problems with geometric flavor. For instance, everybody knows that among any five points within a unit square there exist two at distance at most $\sqrt{2}/2$ apart. (Here and further, "within" a geometric figure means in the interior of that figure, or on its border.) We prefer, however, the following similar exercise.

Problem. Let ten points be arbitrarily placed within an equilateral triangle of side length 3. Prove that there exist two of the ten points that are situated at a distance of at most 1 apart.

Solution. Divide each side of the triangle into three equal parts, then from each point of division draw parallels to the sides of the triangle. Thus we partition the triangle into nine smaller equilateral triangles, each of side 1. We have ten points, thus there are two of them in the same smaller triangle. (If a point belongs to a side common to two smaller equilateral triangles, we consider it in one of those triangles, freely chosen.) It only remains to see that two points within an equilateral triangle are at a distance at most equal to the side of the triangle apart.

Note that the last claim, as obvious as it may seem, needs a proof. Prove it!

Problem. Six points are within a (closed) disk of radius 1. Prove that we can find two of them at a distance of at most 1 apart.

Solution. If there were seven points, the problem's request would follow easily. It would be enough to consider a regular hexagon inscribed in the given circle (the border of the disk); the radii through the vertices of the hexagon partition the disk into six sectors (each with angle of 60°), and, if seven points are given, two of them must be in the same sector, therefore the distance between them is at most 1. (Prove the last statement!) However, we can use this partition of the disk even in our problem's case, when only six points are given. Choose a partition such that one of the six points (call it A) is on one of the radii that realize the partition (and that bound the sectors). If in one of the 60° sectors delimited by that radius there is another point (say B) then A and B are in the same (closed) sector and the distance between A and B is at most 1. Otherwise in those two sectors (that share the radius passing through A) there is none of the five remaining points (other than A), thus these five points are placed in only four sectors. By the pigeonhole principle, two of them share the same sector, and their mutual distance is less than or equal to 1.

A different approach is the following. Draw the radii of the given circle through its center O and each of the given points. There are two of the radii forming an angle of measure at most 60° (since the sum of the six adjacent angles formed by consecutive radii is 360°). Assume that A and B are two of the six points such that the measure of $\angle AOB$ is at most 60°. The triangle AOB, however, also has an angle whose measure is at least 60° (because the measures of the three angles of the triangle sum to 180°, the greatest angle has this property). Suppose (without loss of generality) that $\angle ABO$ has measure greater than or equal to 60°, therefore it also has its measure greater than or equal to the measure of $\angle AOB$. But in a triangle a greater angle is opposite a greater side, thus we finally get $AB \leq OA \leq 1$, as we intended to show.

Note that five points can be chosen within a unit disk such that all their pairwise distances are greater than 1. (How?)

Problem. Show that among any seven points within a triangle of area 1, one can choose three of them such that the area of the triangle they determine is at most $1/4$.

Solution. It would be nice if we had nine points. In that case, due to the generalized pigeonhole principle, three of them would lie in one and the same of the four triangles (each of area $1/4$) determined by the mid-lines of the triangle and its sides, consequently, the triangle they form would be the one we are seeking. Unfortunately, we don't have nine, but only seven points. Fortunately, the above idea works for seven points, too — but we have to be a little more careful. Namely, let ABC be the given triangle, and let M, N, and P be the midpoints of the line segments BC, AC, and AB respectively. We partition the triangle into the triangles BMP, MCN, and the parallelogram $MNAP$. Three of the seven points must be in one of these three regions. If they are within one of the triangles, clearly they determine a triangle with area at most the area of BMP, or MCN, that is, at most $1/4$. But the conclusion is the same if they are within the parallelogram. In this case, we use the following (non-trivial!) statement: the area of a triangle determined by three points within a parallelogram is less than or equal to half the area of the parallelogram. (Prove this claim!) In our case, the area of $MNAP$ is $1/2$, hence three points inside it (or belonging to its sides) determine a triangle with area at most $1/4$, and the solution ends here.

Proposed Problems

1. Prove the assertions that remained unproved in our text, namely:

   a) The distance between any two points within an equilateral triangle is at most equal to the length of the side of the triangle.

   b) The distance between two points within a sector of a disk with angle of 60° is at most equal to the radius of the disk.

   c) The distance between two points within a rectangle is less than or equal to the diagonal of the rectangle. (Although this part has not been proposed in the text, we'll see that a connection exists.)

d) The area of a triangle determined by three points within a parallelogram is less than or equal to half the area of the parallelogram.

2. Prove that among any nine points within a unit square one can find three such that the area of the triangle determined by them is at most 1/8.

3. Let $2n$ $(n \geq 2)$ points be given in the plane and let some line segments joining them be drawn. Prove that if there are at least $n^2 + 1$ segments, then at least one triangle is drawn.

4. Prove that for any integers a, b, c, and d, the number
$$N = abcd(a^2 - b^2)(a^2 - c^2)(a^2 - d^2)(b^2 - c^2)(b^2 - d^2)(c^2 - d^2)$$
is divisible by 7.

5. Prove that from any three integers, one can choose two, say a and b, such that $ab(a - b)(a + b)$ is divisible by 10.

6. Prove that every polyhedron has two faces with the same number of edges.

7. What is the maximum number of bishops that can be placed on a chessboard and that do not attack each other? (Two bishops attack each other if they are on the same diagonal.)

8. On a chessboard 17 rooks are placed. Prove that three of them can be chosen such that they do not attack each other. (Two rooks attack each other if they are in the same row or in the same column of the board.)

9. Let $(G, \cdot)$ be a group with n elements and with identity element e, and let $a_1, a_2, \ldots, a_n$ be elements of G (not necessarily distinct). Prove that the product of some (i.e., one or more) of them is e. (And we don't mean an empty product, automatically considered to be e. However, a product with only one factor is allowed.)

10. Let $(G, \cdot)$ be a finite group and let A and B be subsets of G, such that $|A| + |B| > |G|$ (where $|X|$ denotes the cardinality — the number of elements — of X). Prove that $AB = G$; that is, for every $g \in G$, there exists $a \in A$ and $b \in B$ such that $g = ab$.

11. Let $(G, \cdot)$ be a finite group and let H be a nonempty subset of G closed under multiplication. Prove that H is a subgroup of G.

12. Let $(S, \cdot)$ be a semigroup (that is, the operation "$\cdot$" on S is associative and has an identity element). Prove that any element $s \in S$ has an idempotent power. (That is, for each $s \in S$, there exists a positive integer n such that $(s^n)^2 = s^n$.)

13. Write the complete proof of the (weak) theorem of Schur stating that if the positive integers are partitioned arbitrarily in a finite number of sets, then the equation $x + y = z$ has a solution with all components x, y, and z in the same class of the partition.

14. Prove that $14 \leq S(3) \leq 16$. That is, you must find a partition into three classes of $\{1, \ldots, 13\}$ such that each class of the partition does not contain three numbers x, y, and z such that $x + y = z$ (it is said about such sets that they are *sum-free*), and then prove that in any partition with three classes of $\{1, \ldots, 16\}$ one of the classes is not sum-free.

15. Prove Lagrange's four-square theorem, stating that any natural number can be expressed as the sum of (at most) four perfect squares (numbers like $3 = 1^2 + 1^2 + 1^2$ can be written as the sum of four squares only using a zero).

    a) Prove Euler's four-square identity:

    $$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2)$$
    $$= (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2$$
    $$+(a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1)^2,$$

    thus showing that the product of two (or more) sums of four squares is a sum of four squares, too. Infer that if Lagrange's theorem is true for the primes and for numbers 0 and 1, then it is true for every nonnegative integer.

    Further, let p be an odd prime.

    b) Prove that one can find integers a and b such that

    $$a^2 + b^2 + 1 \equiv 0 \pmod{p},$$

    therefore there exists a (nonzero) multiple of p that can be expressed as the sum of four squares.

    c) Show that, for any integers a and b, the system of congruences

    $$x \equiv az + bt \pmod{p}, \quad y \equiv bz - at \pmod{p}$$

    has a solution (x, y, z, t) in nonnegative integers, not all 0, and all less than $\sqrt{p}$ in absolute value.

    d) Infer that p itself can be written as the sum of four squares.

Solutions

1. a) Let P and Q be any points situated in the interior of the equilateral triangle ABC, or on its border. We can draw the line through P and Q, consider its intersections P' and Q' with the triangle, and we have $PQ \leq P'Q'$, which shows that it suffices to prove the statement only for points on the border of the triangular surface. Thus we can consider, without loss of generality, P and Q to be on the sides of the triangle. Then note that there exists a vertex of the triangle, say A such that the parallel to PQ through A intersects the opposite side (in this case BC) in an interior point of it, say in M, in such a way that $PQ \leq AM$. But $AM \leq AB$ is clear since one of B and C is more remote from the midpoint of BC than M (and the oblique which is further from the perpendicular is longer), hence we have $PQ \leq AM \leq AB$, as desired.

   Actually, based on similar reasoning, one can prove that the maximum distance between two points within an arbitrary triangle is the length of the triangle's longest side.

   b) We consider the sector in a coordinate system with origin in its center (actually the center of the corresponding disk), the x-axis along one of the radii that delimit the sector, and the other one of these radii forming a positive angle of $60°$ with the x-axis. Let M and N be two points within the sector, whose position can be expressed in polar coordinates, or by their complex affixes. Thus we have $z_M = r_M(\cos t_M + i \sin t_M)$, and $z_N = r_N(\cos t_N + i \sin t_N)$ with $r_M = OM$ and $r_N = ON$ in the interval $[0, R]$ (R being the radius of the sector), and with t_M and t_N from the interval $[0°, 60°]$. A simple calculation (or an application of the cosine law) shows that

   $$MN = |z_M - z_N| = \sqrt{r_M^2 + r_N^2 - 2r_M r_N \cos(t_M - t_N)}.$$

   The difference $t_M - t_N$ is in the interval $[-60°, 60°]$, therefore

   $$\cos(t_M - t_N) \geq 1/2,$$

   yielding

   $$r_M^2 + r_N^2 - 2r_M r_N \cos(t_M - t_N) \leq r_M^2 + r_N^2 - r_M r_N.$$

   Now if, for example, $r_M \leq r_N$, we can write

   $$r_M^2 + r_N^2 - r_M r_N = r_N^2 + r_M(r_M - r_N) \leq r_N^2 \leq R^2,$$

and similarly, we prove that the expression under the radical is at most R^2 when $r_N \leq r_M$. Thus, either way,

$$MN = \sqrt{r_M^2 + r_N^2 - 2r_M r_N \cos(t_M - t_N)} \leq \sqrt{r_M^2 + r_N^2 - r_M r_N} \leq R,$$

as we intended to prove.

c) If M and N are points within the rectangle $ABCD$ and P and Q, respectively R and S are the projections of M and N on AB, respectively AD, one readily sees that $MN^2 = PQ^2 + RS^2$, and $PQ \leq AB$, $RS \leq AD$. Thus

$$MN = \sqrt{PQ^2 + RS^2} \leq \sqrt{AB^2 + AD^2} = AC.$$

Clearly, we can have equality only when $\{M, N\} = \{A, C\}$, or $\{M, N\} = \{B, D\}$. In particular, the maximum distance between two points in a square is achieved when the points are opposite corners of the square, and is, of course, the length of the square's diagonal. Actually this does not appear in our text above, but it is useful to prove, for example, that from five points within a unit square there will always be two at distance at most $\sqrt{2}/2$ apart (and this was mentioned in the text).

d) Let X, Y, and Z be points within the parallelogram $ABCD$. The reader can figure out that there is a vertex of the triangle XYZ such that one of the parallels through that vertex to either AB or AD cuts the triangle in two smaller triangles (possibly the parallel coincides with one of the sides of the triangle, and one of the smaller triangles is degenerate, while the other is the initial triangle XYZ). Assume for convenience that the parallel through X to AB intersects the opposite side YZ at the point T, cutting the triangle into two triangular pieces XYT and XZT. Let $d = d(AB, CD)$ be the distance between the parallel lines AB and CD (the height of the parallelogram corresponding to its sides AB and CD). We then have

$$A_{XYZ} = A_{XYT} + A_{XZT} = \frac{1}{2} \cdot XT \cdot d(Y, XT) + \frac{1}{2} \cdot XT \cdot d(Z, XT),$$

where A_{XYZ} is the area of XYZ and $d(Y, XT)$ is the perpendicular distance from Y to XT. Now we have $XT \parallel AB \parallel CD$ and X and T are within the parallelogram, hence $XT \leq AB$ and, also

$$d(Y, XT) + d(Z, XT) \leq d,$$

therefore

$$A_{XYZ} = \frac{1}{2} \cdot XT \cdot (d(Y, XT) + d(Z, XT)) \leq \frac{1}{2} \cdot AB \cdot d = \frac{1}{2} \cdot A_{ABCD},$$

finishing the proof.

2. Partition the square into four little squares with side length $1/2$. We have $9 = 4 \cdot 2 + 1$ points placed in these four little squares, hence three of them are within the same square. By the last part of the previous problem, the area of the triangle determined by them is at most half the area of the little square, that is, at most $1/8$. Of course, the square can be replaced with any parallelogram with area 1, and the result remains true, with the same proof.

3. In other words, a graph with $2n$ vertices and at least $n^2 + 1$ edges must contain a triangle (a complete subgraph with three vertices). We prove this by induction on n. For $n = 2$, let the points A, B, C, and D be given with five of the line segments joining them. Let AB be drawn, and note that either both AC and BC, or both AD and BD are drawn, otherwise, we can only have at most four segments. So, either triangle ABC, or triangle ABD appears. (Observe that the result is also vacuously true for $n = 1$.) Basically the same idea works for the induction step as well.

   Assume the result is true for n, and let $2n + 2$ points be given together with at least $(n + 1)^2 + 1$ segments joining some two of them. Consider again AB to be a drawn segment and look at the set of the other $2n$ points, different from A and B (denote this set by X). If among these points at least $n^2 + 1$ segments are drawn, some three of them form a triangle, by the inductive hypothesis. Otherwise, among them there are at most n^2 segments, thus there are at least $2n+1$ segments joining either A or B with one of the $2n$ points from X. Let $A_1, \ldots, A_k$ be the points from X joined with A, and let $B_1, \ldots, B_l$ be the points from X joined to B. The total number of these points is $k + l = 2n + 1 > 2n$, thus greater than the number of elements of X, to which they all belong, hence there must be two of them that coincide. But the A_is are all distinct, and so are the B_js. The only possibility that remains is that $A_i = B_j$ for some $1 \le i \le k$ and some $1 \le j \le l$. Now, if we denote $C = A_i = B_j$, we have the triangle ABC drawn.

   Note that n^2 segments can be drawn with no triangle appearing; just split arbitrarily the $2n$ points into two sets with n elements each and draw all segments that join a point from one set with a point from the other (thus obtaining a complete bipartite graph on $2n$ vertices). This is a case of Mantel's theorem asserting that the maximum number of edges of a graph on m vertices that does not contain triangles is $[m^2/4]$ (and seems to be another problem that Erdős gave to Pósa in his early years, and Pósa solved it very quickly).

4. If one of the four numbers a, b, c, d is divisible by 7, the conclusion is straightforward. Otherwise, they are congruent to ± 1, ± 2, or ± 3 modulo

7, hence their squares are congruent to either of 1, 4, or 2 modulo 7. So, we have four squares, and only three possible remainders for them when divided by 7. By the pigeonhole principle, there are two squares among a^2, b^2, c^2, and d^2 giving the same remainder at division by 7. Then their corresponding difference is divisible by 7, and so will be N.

5. Clearly $xy(x-y)(x+y)$ is even for all integers x and y (it is actually divisible by 4 when x and y have the same parity), so it remains to prove that, given three integers, there are two among them, a and b, such that $ab(a-b)(a+b)$ is divisible by 5. This is clearly true if at least one of the given numbers is divisible by 5, hence we can assume further that none of those numbers is divisible by 5. Looking at the remainders of the numbers divided by 5 the problem is now the following: if three numbers are given from the set $\{1,2,3,4\}$, there exist two among them, a and b such that either $a-b$, or $a+b$ is divisible by 5. Since this is clear if two of the given numbers are equal, the problem transforms again into: if three *distinct* numbers are given from the set $\{1,2,3,4\}$, there exist two among them, a and b such that $a+b$ is divisible by 5. Indeed, we have three numbers and only two sets $\{1,4\}$ and $\{2,3\}$ to which they belong, hence both numbers from one of these sets has to be among the three numbers, and the sum of these numbers is 5.

   This was proposed by Ioan Tomescu for a Romanian TST in the eighties of the former century.

6. The polyhedron has a face F with the greatest number of edges; let this number be n. Then each of the n faces that share an edge with F can have a number of edges from 3 to n; by the pigeonhole principle, two of these faces have the same number of edges.

   One can prove similarly that in any convex polyhedron, there exist two vertices from which the same number of edges emerge. Just choose the vertex V from which the greatest number of edges emerge. From any other vertex, a number of 3, or 4, etc, until n edges can start, so there are two vertices incident with the same number of edges.

7. There are 7 black diagonals (formed with only black squares) on the chessboard (the "great" one, from a1 to h8, and the parallels to it: from c1 to h6, and so on), and also there are 7 white diagonals (the big one from a8 to h1); these 14 diagonals contain all the squares of the board. So, if 15 bishops are placed on the board, two of them are on the same diagonal, therefore they threaten each other. Thus the maximum required number is at most 14.

   On the other hand, there exists an arrangement of 14 non-attacking bishops: just put 8 of them in the squares of the first row (from a1 to a8), and the other six in the last row, in the squares from h2 to h7. So the maximum number of non-attacking bishops is precisely 14.

The similar problem with rooks is somehow simpler: solve it. (Rooks attack each other if they are in the same row, or in the same column of the board.)

8. **Solution I.** There are $17 = 8 \cdot 2 + 1$ rooks and only 8 columns on the board, thus we can choose three of the rooks situated in the same column; name this column C_1. In C_1 at most 8 rooks can be placed, so there remain at least 9 rooks in the seven columns other than C_1. By the pigeonhole principle, there exists one of these columns (let it be C_2) that contains at least two rooks. Of course, there are at most 16 rooks in C_1 and C_2, therefore at least one rook remains in the six columns different from C_1 and C_2. Call C_3 the column (different from both C_1 and C_2) that contains at least one rook R_1. Because in C_2 there are at least two rooks, we can choose one of them (and we name it R_2) that is placed in a row different from the row containing R_1. Finally, because C_1 has at least three rooks, we can choose one of them (R_3) that is situated in a row different from the rows of R_1 and R_2. Clearly, any two of the rooks R_1, R_2, and R_3 are in the different columns C_3, C_2 and C_1 respectively and they are in different rows too, hence they do not attack each other.

   Solution II. Glue together two opposite sides of the chessboard in such a manner that it becomes cylindrical. Follow the chains of squares of the same color on the surface of the cylinder thus obtained: there are eight such chains, each consisting of eight squares. Since $17 = 8 \cdot 2 + 1$, three rooks are placed in squares belonging to the same such chain, and these rooks do not threaten each other in the initial position (on the board).

   This is a variant of a well-known (among those interested in mathematical contests) problem of Alexander Soifer: if 41 rooks are placed in the squares of a 10×10 chessboard, then one can choose five of them that do not attack each other. The reader will now be able to solve this problem by either of the two ingenious methods described above.

9. If any of the elements a_1, $a_1a_2, \ldots$, $a_1a_2 \cdots a_n$ equals e, we are done. Otherwise, we have n elements that belong to the set $G \setminus \{e\}$ with only $n-1$ elements, hence two of them must be equal. This means that there exist $1 \le i < j \le n$ such that $a_1 \cdots a_i = a_1 \cdots a_j$. By simplifying to the left with $a_1 \cdots a_i$ (observe that there is no need for commutativity) we remain with $e = a_{i+1} \cdots a_j$, and our job is done.

   The reader surely recognized the *very* well-known problem stating that from any n integers one can choose some of them whose sum is divisible by n (which can be obtained from the general enounce by specializing to the group of residue classes modulo n; of course, the fact that this is an additive group doesn't matter at all).

10. The set $AB = \{ab \mid a \in A,\ b \in B\}$ is included in G, so only the opposite inclusion has to be proven. For this scope, let g be any element of G. The elements of A are all distinct and their number is $|A|$. Also, the products of g with the inverses of the elements of B are all mutually distinct, and their number is $|B|$. Together these two sets (A and gB^{-1}) have $|A| + |B|$ elements, thus, by hypothesis, the union of these two sets has more elements than G. By the pigeonhole principle one element $a \in A$ must equal one element $gb^{-1} \in gB^{-1}$. But $a = gb^{-1}$ multiplied to the right with b gives $ab = g$, that is, $g \in AB$.

    For example, specializing again to the group $(\mathbb{Z}_n, +)$ of the residue classes modulo n, the following statement can be obtained (after being rephrased in the language of remainders): if A and B are two sets of integers with $|A| + |B| > n$, then the elements $a + b$, with $a \in A$ and $b \in B$ give all possible remainders (from 0 to $n - 1$) when divided by n.

11. Because H is given to be closed under the operation of G, it remains to prove that it is also closed under taking the inverse (and of course, that it contains the identity element e of G). Let h be any element of H; its powers $h, h^2, \ldots$ are infinitely many elements in the finite set G. By the infinite case of the pigeonhole principle, there must exist two of them with distinct exponents that are equal. Say, for example, that $h^m = h^{m+p}$, with positive integers m and p. Multiplying by $(h^m)^{-1}$, we get $h^p = e$, thus e belongs to H (as H is closed under multiplication). Also this equality shows that the inverse of h is h^{p-1} (since $hh^{p-1} = h^{p-1}h = e$), therefore it also belongs to H, for the same reason as before.

12. The first part of the previous solution can be repeated here in order to conclude that if $s \in S$, we have $s^m = s^{m+p}$ for some positive integers m and p (but we cannot do the cancelation). It follows inductively that $s^{m+kp} = s^m$ for every positive integer k, then (by multiplying with s^n) that $s^{m+n+kp} = s^{m+n}$ for every positive integers k and n. Now choose k big enough to have $kp > m$, and choose $n = kp - m$, then observe that the above equality becomes $s^{2kp} = s^{kp}$, meaning that s^{kp} is the idempotent power of s that we were looking for. (Actually, the solution shows that there are infinitely many such powers of s.)

13. As previously discussed, we call a set of numbers *sum-free* if it does not contain three numbers x, y, and z such that $x + y = z$. Of course, a sum-

free set is also difference free, in the obvious sense that the difference $u - v$ of two of its members cannot be another member w of the set (since in that case $u = v + w$ with all u, v, and w from the set). We proceed by contradiction, so let the positive integers be partitioned as $\mathbb{N}^* = C_1 \cup \cdots \cup C_k$ in such a manner that all classes $C_1, \ldots, C_k$ are sum-free. Because there are infinitely many elements into finitely many classes, one of the classes has to contain infinitely many of the positive integers. Without loss of generality, assume that C_1 is infinite, and let $a_1^{(1)} < a_2^{(1)} < \cdots$ be the elements of C_1. By our assumption, C_1 is sum-free, hence none of the differences $a_2^{(1)} - a_1^{(1)} < a_3^{(1)} - a_1^{(1)} < \cdots$ belongs to C_1, therefore they must be in $C_2 \cup \cdots \cup C_k$. Again, by the infinite case of the pigeonhole principle, there is one of $C_2, \ldots, C_k$ containing infinitely many of the above differences. Suppose this set is C_2 and denote those differences that belong to C_2 by $a_1^{(2)} < a_2^{(2)} < \cdots$ (in increasing order). Observe that the numbers $a_2^{(2)} - a_1^{(2)} < a_3^{(2)} - a_1^{(2)} < \cdots$ are differences between some elements of C_2 by their very definition, but also they are differences between numbers of C_1. Indeed, there exists an increasing set of positive integers $2 \le i_1 < i_2 < \cdots$ such that $a_j^{(2)} = a_{i_j}^{(1)} - a_1^{(1)}$ for all j, therefore $a_j^{(2)} - a_1^{(2)} = a_{i_j}^{(1)} - a_{i_1}^{(1)}$ for all j. Consequently, by our contrapositive assumption, these differences (which are positive integers, nevertheless) have to be in $C_3 \cup \cdots \cup C_k$, hence infinitely many of them belong to, let us say, C_3. Denote by $a_1^{(3)} < a_2^{(3)} < \cdots$ those of the differences $a_2^{(2)} - a_1^{(2)} < a_3^{(2)} - a_1^{(2)} < \cdots$ that belong to C_3 and observe that the new differences $a_2^{(3)} - a_1^{(3)} < a_3^{(3)} - a_1^{(3)} < \cdots$ are differences between elements of C_3, but also differences between elements of C_2 and differences between elements of C_1. Our assumption shows that they cannot be in any of C_1, C_2, or C_3, so infinitely many of them belong to C_4 (if necessary, change the indices of the classes in order to go on like this) — we denote them by $a_1^{(4)} < a_2^{(4)} < \cdots$, then take their differences $a_2^{(4)} - a_1^{(4)} < a_3^{(4)} - a_1^{(4)} < \cdots$, and so on. By this process, we build infinite sequences $a_1^{(l)} < a_2^{(l)} < \cdots$ of elements from C_l, for any $1 \le l \le k$ with the property that the differences $a_2^{(l)} - a_1^{(l)} < a_3^{(l)} - a_1^{(l)} < \cdots$ are differences not only between the elements of C_l, but also between elements of every C_j with $1 \le j \le l$ (and for every $1 \le l \le k$). Thus the last such differences that we get, namely $a_2^{(k)} - a_1^{(k)} < a_3^{(k)} - a_1^{(k)} < \cdots$ are differences between elements of each and every C_j, $1 \le j \le k$, thus our assumption leaves them no room in any of the classes $C_1, \ldots, C_k$ of the partition, which, of course, is absurd.

14. An example of a partition of $\{1, \ldots, 13\}$ into three sum-free subsets is

$$\{1, \ldots, 13\} = \{1, 4, 10, 13\} \cup \{2, 3, 11, 12\} \cup \{5, 6, 7, 8, 9\}$$

and thus $S(3) \geq 14$. (Recall that $S(3)$ is the smallest positive integer S such that in any partition with three classes of $\{1, \ldots, S\}$ there exist one of the classes which is not sum-free.)

Now let $\{1, \ldots, 16\} = A \cup B \cup C$ be a partition with three classes of $\{1, \ldots, 16\}$ and assume, by way of contradiction, that each of A, B, and C is sum-free (the proof is very similar to the previous one). One of A, B, C has at least 6 elements, by the pigeonhole principle. Without loss of generality, we can consider that $a < b < c < d < e < f$ are all in A. Look at the five differences $b - a < c - a < d - a < e - a < f - a$: due to our presupposition, they are all in $B \cup C$. By the pigeonhole principle again, at least three of them are in one and the same of these sets. Again, without loss of generality, we can consider that B is the set that contains at least three of them, and that these three are $b - a$, $d - a$, and $e - a$. Because they are in B, which is assumed to be sum-free, the differences $(d - a) - (b - a) = d - b$ and $(e - a) - (b - a) = e - b$ are not in B — but they are not in A either, as A is sum-free, too. So, necessarily, $d - b$ and $e - b$ are in C, and now their difference

$$(e - b) - (d - b) = (e - a) - (d - a) = e - d$$

has no place in any of A, B, and C, which is false because $e - d$ is a positive integer, smaller than e, hence smaller than 16 (thus it has to be in one of these sets of the partition).

Thus $S(3) \leq 16$, and, actually, $S(3)$ is 14, 15, or 16. To prove the exact value $S(3) = 14$ requires some more work, based on the analysis of many cases, and doing it here is not our goal. However, the interested reader will surely be able to prove that $S(2) = 5$ (and that $S(1) = 2$, of course!).

15. a) Except from the fact that, for real numbers $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4$, the identity just says that the product of norms of two quaternions is equal to the norm of their product, a solution based on elementary algebra can be readily given (and it shows the identity to be valid for all $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4$ being elements of a commutative ring). We expand the squares from the right hand side with the formula

$$(a + b + c + d)^2 = a^2 + b^2 + c^2 + d^2 + 2ab + 2ac + 2ad + 2bc + 2bd + 2cd$$

and get the left hand side expression by collecting all sixteen squares thus obtained (starting with $a_1^2 b_1^2$ and finishing with $a_4^2 b_1^2$). The reader can surely check that all other terms from the right hand side expansions cancel each other, hence the identity is true as stated.

It follows then by an easy and canonical induction that the product of any finite number of numbers, each of which can be written as the sum of four squares can also be expressed as the sum of four squares. Since any integer greater than 1 is the product of a few primes, the theorem would follow if we had it proved for primes (which we will do later).

b) There are $(p+1)/2$ distinct squares modulo p. Indeed, we can have $u^2 \equiv v^2 \pmod{p}$ if and only if $(u-v)(u+v) \equiv 0 \pmod{p}$, that is, if and only if p divides either $u-v$, or $u+v$. So, $0^2, 1^2, \ldots, ((p-1)/2)^2$ are all distinct modulo p (because if $0 \le u, v \le (p-1)/2$, $u+v$ cannot be divisible by p, unless $u = v = 0$, while $u-v$ can be divisible by p only when $u = v$; thus, either way, $u^2 \equiv v^2 \pmod{p}$ implies $u = v$). The squares from $((p+1)/2)^2$ to $(p-1)^2$ repeat the values of $1^2, \ldots,$ $((p-1)/2)^2$ since $(p-j)^2 \equiv j^2 \pmod{p}$, thus there are exactly $(p+1)/2$ different squares modulo p. Now the integers

$$0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

are all distinct modulo p, and the same can be said about

$$-0^2-1, -1^2-1, \ldots, -\left(\frac{p-1}{2}\right)^2-1.$$

However, together, the above numbers form a set of $p+1$ integers, so (by the pigeonhole principle) there are two of them congruent modulo p. Clearly, it must be a number from the first sequence congruent to a number from the second one, thus there exist a and b (both from $\{0, 1, \ldots, (p-1)/2\}$, but this won't matter further) such that

$$a^2 \equiv -b^2 - 1 \pmod{p} \Leftrightarrow a^2 + b^2 + 1 \equiv 0 \pmod{p},$$

and we arrived at the desired conclusion: for some integers a and b, a^2+b^2+1 is a multiple of p — or we can say that some nonzero multiple of p can be written $a^2+b^2+1^2+0^2$, that is, as the sum of four squares. Usually the proof goes on by showing that the smallest nonzero multiple of p having this property is exactly p, but we will proceed in a different manner.

c) This is very similar to the proof of Thue's theorem.
Consider all pairs of integers of the form $(m-ap-bq, n+aq-bp)$, where m, n, p, and q all run through the set $\{0, 1, \ldots, [\sqrt{p}]\}$, thus a total of $([\sqrt{p}]+1)^4 > (\sqrt{p})^4 = p^2$ such pairs. Because there are only p^2

possibilities for a pair of integers taken modulo p, there must exist (by the pigeonhole principle) two quadruples of integers

$$(m_1, n_1, p_1, q_1) \neq (m_2, n_2, p_2, q_2)$$

such that

$$(m_1 - ap_1 - bq_1, n_1 + aq_1 - bp_1) \text{ and } (m_2 - ap_2 - bq_2, n_2 + aq_2 - bp_2)$$

are equal modulo p. But then the integers $x = m_1 - m_2$, $y = n_1 - n_2$, $z = p_1 - p_2$, and $t = q_1 - q_2$ are not all zero, less than $\sqrt{p}$ in absolute value, and they verify the congruences

$$x \equiv az + bt \pmod{p}, \; y \equiv bz - at \pmod{p}$$

as desired.

d) Now it's time to finalize the proof of Lagrange's theorem. For a and b with the property $a^2 + b^2 + 1 \equiv 0 \pmod{p}$, there exist integers $0 \leq x, y, z, t < \sqrt{p}$, not all 0, satisfying the above congruences. It follows that

$$x^2 + y^2 \equiv (az - bt)^2 + (bz - at)^2 = (a^2 + b^2)(z^2 + t^2) \pmod{p};$$

nevertheless, $a^2 + b^2 \equiv -1 \pmod{p}$, hence the previous congruence becomes

$$x^2 + y^2 \equiv -(z^2 + t^2) \pmod{p} \Leftrightarrow x^2 + y^2 + z^2 + t^2 \equiv 0 \pmod{p}.$$

Thus, there is a multiple $sp = x^2 + y^2 + z^2 + t^2$ of p that can be expressed as the sum of four squares; because x, y, z, t are not all zero, and they are smaller than $\sqrt{p}$, it follows that s can be only 1, 2, or 3. Of course, if $s = 1$ we are done. Note that at least two of x, y, z, and t have the same parity (the pigeonhole principle, once again!) — let them be x and y — thus, for $s = 2$, the equality

$$2p = x^2 + y^2 + z^2 + t^2$$

implies that z and t must have the same parity. Then we have

$$p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2$$

and p is written as the sum of four squares of integers.

Finally, let $s = 3$. Hence, we have

$$3p = x^2 + y^2 + z^2 + t^2.$$

The square of an integer u is either 0 modulo 3 (if u is divisible by 3, too), or 1 modulo 3 (if $u \equiv \pm 1 \pmod{3}$), thus we can have one of two situations: either x, y, z, and t are all divisible by 3, or exactly one of them is so. Let x be divisible by 3, and note that y, z, and t are either all congruent to 0, or all of them congruent to ± 1 modulo 3, hence we can assume (by changing their signs in the second case if necessary) that $y \equiv z \equiv t \pmod{3}$. In this case, we get the following expression of p as the sum of four integer squares:

$$p = \left(\frac{y+z+t}{3}\right)^2 + \left(\frac{x+y-z}{3}\right)^2 + \left(\frac{x+z-t}{3}\right)^2 + \left(\frac{x+t-y}{3}\right)^2$$

and the proof is now complete. (Of course, for a complete proof, don't forget to check that 0, 1, and 2 are expressible as sums of four squares!)

Chapter 2

A Property of the Greatest Common Divisor

The greatest common divisor of two or more natural numbers is precisely what its name says, that is: the greatest of the common divisors of those numbers. For instance, the (natural) divisors of 12 are 1, 2, 3, 4, 6, and 12, and the divisors of 18 are 1, 2, 3, 6, 9, and 18. We see that 1, 2, 3, and 6 are the divisors of both 12 and 18 (their *common* divisors), thus the greatest common divisor of 12 and 18 is 6. We write this as $\gcd(12,18) = 6$, or simply $(12,18) = 6$. The correct definition in the natural frame of the integers is in most cases equivalent to the above one, which, however, cannot be used in similar structures (as the polynomials, for example) where a theory of divisibility can be developed.

Observe that $6 = (12,18) = 18 - 12$, or $6 = (12,18) = 2 \cdot 12 - 18$, and that other expressions of 6 in the form $12x + 18y$, with integers x and y are also available (find more of them!). In general, for any integers a and b, and for their greatest common divisor d, there exist (not uniquely determined, but rather infinitely many pairs of) integers x and y such that $d = ax + by$. This is the property of the greatest common divisor that we are concerned with in this chapter. Maybe we should have called it *the most important* property of the greatest common divisor, but we do not intend to be so categorical about such theoretical issues. Nevertheless, we will try to see the power of this property in solving various problems – but first let us recall some basic facts about divisibility.

Let a and b be two integers. We say that a *is divisible* by b (or that b *divides* a, or that a is a *multiple* of b, or that b is a *divisor* of a), and we denote this by $a \,\vdots\, b$ or $b \mid a$ if there exists an integer c such that $a = bc$. When $b \neq c$ this is equivalent to saying that the remainder of a when divided by b is zero. For instance, 343 is divisible by 7, as $343 = 7 \cdot 49$, while 343 is not divisible by 8, the remainder of the division of 343 by 8 being $7 \neq 0$. When $b = 0$, only $a = 0$ is possible (the only multiple of 0 is 0, although every integer is a divisor of 0). The following simple (but useful) properties are left to the reader for proof (all variables that appear in the statement represent integers).

Proposition. *We have (where all variables represent integers):*

a) For nonzero b, a is divisible by b if and only if the remainder of the Euclidean division of a by b is 0.

b) If $a \vdots b$ and $a \neq 0$, then $|a| \geq |b|$.

c) $a \mid 0$, $1 \mid a$, $a \mid a$ (reflexivity), and if $a \mid b$ and $b \mid c$, then $a \mid c$ (transitivity).

d) If $a \mid b$ and $b \mid a$, then either $a = b$ or $a = -b$. (We say that a and b are associates.*)*

e) If $d \mid a_i$ for each $1 \leq i \leq n$, then d also divides $b_1a_1 + \cdots + b_na_n$. In particular, a common divisor of a and b divides both their sum and their difference.

A *greatest common divisor* of integers $a_1, \ldots, a_n$ is an integer d that divides each of them and has also the following maximality (in the sense of divisibility) property: whenever d' is a common divisor of $a_1, \ldots, a_n$, d' has to divide d. It turns out that, in general, there are two integers with these properties, which are associates. The convention is to choose the positive one of them, call it *the* greatest common divisor of $a_1, \ldots, a_n$, and denote it by $\gcd(a_1, \ldots, a_n)$, or, as will we do further, just $(a_1, \ldots, a_n)$. For instance $(12, 18) = 6$ (as we have already seen), but -6 also satisfies both properties from the definition of the greatest common divisor for the integers $a_1 = 12$ and $a_2 = 18$. This is not a problem, since the properties of associates (related to divisibility) are the same. Notice yet that the greatest common divisor of a and b is $|a|$ whenever a is a divisor of b; in particular $(1, a) = 1$, and $(a, a) = |a|$ for every integer a. (The reader is invited to generalize these equalities to the case of n integers.) This includes the case $(0, 0) = 0$; just do carefully apply the definition in order to see that 0 is the only possible value for $(0, \ldots, 0)$, with no matter how many zeros — although in some books this is not defined.

Similarly, a least common multiple m of the integers $a_1, \ldots, a_n$ is a common multiple of them that also has the property: if m' is also a common multiple of $a_1, \ldots, a_n$, then $m \mid m'$. *The* least common multiple is the positive integer among the two associates with these properties, and we will denote it by $\operatorname{lcm}(a_1, \ldots, a_n)$, or simply by $[a_1, \ldots, a_n]$ (with square brackets). For example, $[12, 18] = 36$ as one can immediately check only by enumerating the first few multiples of 12 and 18. Note that the least common multiple of some nonzero $a_1, \ldots, a_n$ is nonzero by its very definition (because $a_1 \cdots a_n$ is a nonzero common multiple, and 0 does not divide any nonzero number), although 0 is a common multiple for all integers. However, when among the a_is there is at least one equal to 0, the least common multiple must be considered to be 0, since 0 is the only common multiple of all numbers in that case. Note that if some numbers in the sequence $a_1, \ldots, a_n$ are replaced by their associates, the greatest common divisor and the least common multiple do not change. Thus $(-12, 18) = (12, 18) = 6$ and $[-12, -18] = [12, 18] = 36$. Yet, if we change the order of numbers in the sequence, the greatest common divisor and least common multiple remain the same. Also note that if a is a divisor of b, then $(a, b) = |a|$ (as mentioned above) and $[a, b] = |b|$; in particular, $(a, 1) = 1$, $[a, 1] = |a|$, $(a, 0) = |a|$, and $[a, 0] = 0$.

The primes are the numbers $2, 3, 5, 7, 11, \ldots$, or, referring to integers, $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$. An integer p is called a prime if it is not equal to either of -1, 0, 1, and its *only* divisors are ± 1 and $\pm p$ (observe that any integer k is divisible by ± 1 and $\pm k$). In other words, p is a prime if its only expressions as the product of two integers are $p = 1 \cdot p = (-1) \cdot (-p)$, or if an equality $p = ab$ (with integers a and b) necessarily implies that one of the factors a and b is associate to p. The following result is very important.

Theorem. *Every integer different from -1, 0, and 1 can be uniquely expressed as the product of prime factors. More precisely, if $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$, there exist distinct positive primes $p_1, \ldots, p_k$ and positive integers $a_1, \ldots, a_k$ such that*

$$n = \pm p_1^{a_1} \cdots p_k^{a_k}.$$

If $n = \pm q_1^{b_1} \cdots q_l^{b_l}$ is another such representation of n with $q_1, \ldots, q_l$ positive primes, and $b_1, \ldots, b_l$ positive integers, then $k = l$ and $p_1, \ldots, p_k$ coincide in some order with $q_1, \ldots, q_l$, and $a_1, \ldots, a_k$ coincide, in the same order, with $b_1, \ldots, b_l$. (If the primes are not chosen to be positive then $p_1, \ldots, p_k$ are associate to $q_1, \ldots, q_l$ in some order.)

This is *the fundamental theorem of arithmetic* (so you can see its importance from its very name), and it speaks about representations like $12 = 2^2 \cdot 3$, $343 = 7^3$, or $-100 = -2^2 \cdot 5^2$, so that it basically says that every integer (except -1, 0, and 1) can be uniquely written as a product of primes. Of course you can say that $12 = 2 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 2 = 2 \cdot 3 \cdot 2$, but these decompositions do not differ essentially.

One of the (many) uses of the fundamental theorem of arithmetic, is for computing the greatest common divisor and the least common multiple of a set of integers. We recall here the (well-known) result for two integers, but it works analogously for any finite (or infinite, sometimes) set of numbers. First, let us observe that we can express the factorization of an integer into primes in the following manner, too. Let $p_1 = 2$, $p_2 = 3$,... be the sequence of positive primes. Then any integer m different from $-1, 0$, and 1 can be represented as

$$m = \pm \prod_{i \geq 1} p_i^{a_i}$$

for some nonnegative integers $a_1, a_2, \ldots$ from which only finitely many are nonzero. We then have the following:

Proposition. *Let* $m = \pm\prod_{i\geq 1} p_i^{a_i}$, *and* $n = \pm\prod_{i\geq 1} p_i^{b_i}$ *be the factorizations of two integers* m *and* n, *where* $m, n \notin \{-1, 0, 1\}$ *and the* a_i*s and* b_i*s are nonnegative integers, with only finitely many of the* a_i*s and only finitely many of the* b_i*s being nonzero. Then*

$$(m,n) = \prod_{i\geq 1} p_i^{\min\{a_i,b_i\}}$$

and

$$[m,n] = \prod_{i\geq 1} p_i^{\max\{a_i,b_i\}}.$$

Thus

$$(12,18) = (2^2 \cdot 3, 2 \cdot 3^2) = 2^{\min\{2,1\}} \cdot 3^{\min\{1,2\}} = 2 \cdot 3 = 6,$$
$$[12,18] = [2^2 \cdot 3, 2 \cdot 3^2] = 2^{\max\{2,1\}} \cdot 3^{\max\{1,2\}} = 2^2 \cdot 3^2 = 36.$$

Using the fundamental theorem of arithmetic, we immediately get the following properties for the greatest common divisor and least common multiple.

Corollary. *a) We have* $(a, na + b) = (a, b)$ *for integers* a, b, *and* n *(we do not need the fundamental theorem for this one).*

b) If a *and* b *are relatively prime (that is, their greatest common divisor is 1), then* $(a,c)(b,c) = (ab,c)$.

c) If a *and* b *are relatively prime and* $a \mid bc$, *then* $a \mid c$.

d) For all integers a *and* b, *we have*

$$(a,b)[a,b] = |ab|.$$

These are also important properties of the greatest common divisor and least common multiple, although their proofs are simple (and we leave them to the reader). The last part says that the product of the greatest common multiple and least common multiple of *two* integers equals the absolute value of their product (equals their product for natural numbers). For example, $6 \cdot 36 = 12 \cdot 18$, but beware! This is not at all true for more than two numbers: even though $(2,3,5)[2,3,5] = 2 \cdot 3 \cdot 5$, a slight change makes the equality untrue: $(2,3,6)[2,3,6] = 1 \cdot 6 = 6 \neq 2 \cdot 3 \cdot 6$ (and this happens in many cases). However, relations between numbers and their greatest common divisor and least common multiple can be found, such as

$$[a,b,c](a,b)(a,c)(b,c) = abc(a,b,c)$$

or

$$[a, b, c](ab, ac, bc) = abc.$$

Try to prove these by using the factorizations of the numbers and of their greatest common divisor and least common multiple!

It is time for the main character of the chapter, so we state and prove the property of the greatest common divisor that we announced in the title.

Theorem. *Let $a_1, \ldots, a_n$ be integers, and let d be their greatest common divisor. Then d is a linear combination of $a_1, \ldots, a_n$; that is, there exist integers $x_1, \ldots, x_n$ such that*

$$d = a_1x_1 + \cdots + a_nx_n.$$

Proof. Let $I = \{a_1z_1 + \cdots + a_nz_n \mid z_1, \ldots, z_n \in \mathbb{Z}\}$ be the set of all possible linear combinations with integer coefficients of $a_1, \ldots, a_n$ (I is called the *ideal* generated by $a_1, \ldots, a_n$). Clearly, any element of I is divisible by d (see the first proposition).

If $a_1 = \cdots = a_n = 0$, the result is clear (as $d = 0$), so we may assume that there are nonzero numbers among $a_1, \ldots, a_n$, in which case, I does not reduce to $\{0\}$. Let c be the least positive element of I (if $x \in I$, then $-x \in I$, too, hence there must be positive elements in I). Thus c itself (as any member of I) is divisible by d. We show that d is also divisible by c, which will give us $c = d$ (because they are both positive and associates).

Indeed, let $a_1 = cq + r$, where q and r are the respective quotient and remainder left upon dividing a_1 by c.

We have $c \in I$, therefore $c = a_1z_1 + \cdots + a_nz_n$ for some integers $z_1, \ldots, z_n$, consequently

$$r = a_1 - cq = a_1(1 - z_1q) + a_2(-z_2q) + \cdots + a_n(-z_nq)$$

belongs to I. But $r < c$ and c is the smallest positive integer from I, hence $r = 0$ is the only possibility, showing that c divides a_1. Similarly, we get that c is a divisor of every a_i, therefore c is a divisor of d. As we said above $d = c$ follows, hence d belongs to I, thus being a linear combination of $a_1, \ldots, a_n$, as we intended to prove.

Corollary. *a) Let $a_1, \ldots, a_n$ be relatively prime integers (that is, their greatest common divisor is 1). Then there exist integers $x_1, \ldots, x_n$ such that*

$$a_1x_1 + \cdots + a_nx_n = 1.$$

b) If $d = (a_1, \ldots, a_n)$, then for an integer k, there exist integers $v_1, \ldots, v_n$ such that

$$a_1v_1 + \cdots + a_nv_n = k$$

if and only if d divides k.

Proof. The first part is obvious. For the second observe that if $a_1v_1+\cdots+a_nv_n = k$, then any common divisor of $a_1, \ldots, a_n$ (including d) must also be a divisor of k. For the converse, note that, by the theorem, we can find integers $x_1, \ldots, x_n$ such that $a_1x_1 + \cdots + a_nx_n = d$. Then for $v_i = (k/d)x_i$ (which are integers, as k is divisible by d), we clearly have $a_1v_1 + \cdots + a_nv_n = k$.

We also have the following:

Proposition. *Let a and b be positive relatively prime integers. Then there exist positive integers u and v such that $au - bv = 1$.*

Proof. The numbers ax with $x = 0, 1, \ldots, b-1$ are mutually distinct modulo b, that is, their remainders when divided by b are distinct, and the number of such remainders is, of course, b. So, they form a *complete residue system* modulo b, that is, they provide all possible remainders of division by b. (Indeed, if $ax \equiv ay \pmod{b}$ for some $x, y \in \{0, 1, \ldots, b-1\}$, then b divides $a(x-y)$, thus b divides $x-y$, since b is relatively prime to a. But $|x-y| < b$ and $b \mid x-y$ imply $x = y$.) So, there must exist some $u \in \{0, 1, \ldots, b-1\}$ (and one sees immediately that actually u cannot be 0, except for the case $b = 1$) such that $au \equiv 1 \pmod{b}$, that is, such that $au - 1$ is divisible by b. Thus we have $au - 1 = bv$, which was to prove. For $a = 1$ we get $u = 1$, too, and $au - 1$ is 0, also yielding $v = 0$. Nevertheless, in this case we can find many pairs of *positive* integers u and v such that $au - 1 = u - 1 = bv$ (for example, $u = b+1$ and $v = 1$). Similarly we deal with the case $b = 1$. When $a \geq 2$ and $b \geq 2$ we get $au - 1$ a positive integer, and v will be a positive integer, too.

Note that for $a \geq 2$ and $b \geq 2$ we can choose u such that $0 < u < b$ (and v such that $0 < v < a$). Also note that this proposition can be the starting point of a new proof of the main theorem (we leave this as an exercise for the reader; see the proposed problems, too). Also observe that we have the following:

Corollary. *Let n be a positive integer. In the ring $\mathbb{Z}/n\mathbb{Z}$, an element $\overline{x}$ is invertible if and only if x is relatively prime to n. We denoted by $\overline{x}$ the residue class of the integer x modulo b.*

Proof. If $\overline{x}$ is invertible, there exists $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{xy} = \overline{1}$, that is, $xy - 1$ is divisible by n or $xy - 1 = nz$, for some integer z. Obviously this implies that any common divisor of x and n divides 1, too.

Conversely, if x and n are relatively prime, there are integers u and v such that $xu - nv = 1$, and this yields $\overline{xu} = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$, which we wanted to prove.

After acknowledging the above theorem and its corollary, a natural question arises: given integers $a_1, \ldots, a_n$ and k, *how* can we find integers $v_1, \ldots, v_n$ such that $a_1v_1 + \cdots + a_nv_n = k$? (Of course, in the case when the equation $a_1x_1 + \cdots + a_nx_n = k$ is solvable in integers.) And, moreover, we can ask whether and how we can find *all* the solutions of the equation $a_1x_1 + \cdots + a_nx_n = k$ in the integers.

For a simple starting example, let us look at the equation $5x + 7y = 3$.

It definitely has solutions, because $(5, 7) = 1$ is a divisor of 3, but how do we find at least one such solution? The most natural (although naïve) way is to replace x by concrete values until we find one such that $5x - 3$ is a multiple of 7 (or, such that $5x \equiv 3 \pmod 7$). As we have seen in the above proposition, we need make at most 6 trials: one of the numbers $5 \cdot 1 - 3$, $5 \cdot 2 - 3$, $5 \cdot 3 - 3$, $5 \cdot 4 - 3$, $5 \cdot 5 - 3$, $5 \cdot 5 - 3$, and $5 \cdot 6 - 3$ must be divisible by 7. Indeed, we get $5 \cdot 2 - 3 = 7 \Leftrightarrow 5 \cdot 2 + 7 \cdot (-1) = 3$, hence the pair $x_0 = 2$, $y_0 = -1$ is a solution of our equation.

Now, a pair (x, y) of integers is a solution of the equation if and only if

$$5x + 7y(= 3) = 5x_0 + 7y_0, \quad \text{or} \quad 5(x - x_0) = -7(y - y_0).$$

Since 5 and 7 are relatively prime this can only happen if $x - x_0 = 7t$ and $y - y_0 = -5t$, for some integer t. Thus all the solutions of the equation $5x + 7y = 3$ in integers are given by the formulae $x = x_0 + 7t = 2 + 7t$, $y = y_0 - 5t = -1 - 5t$, for some integer t.

Although this method is far from being the best for finding a solution of the equation $ax + by = c$ (since we might need to do all $b - 1$ verifications for $x \in \{1, \dots, b - 1\}$, and b can be large enough to make this task very unpleasant), the reader can easily see that finding all solutions still works in the same way for any equation $ax + by = c$, where a and b are relatively prime. (Clearly, it suffices to consider only the case when $(a, b) = 1$, as otherwise we can reduce the equation — if it is solvable — to the form $a_1x + b_1y = c_1$, where $a_1 = a/(a, b)$, $b_1 = b/(a, b)$, $c_1 = c/(a, b)$, and $(a_1, b_1) = 1$.) Namely we have the following result, for which the reader will surely find his or her own proof.

Proposition. *Let a, b, and c be positive integers such that a and b are relatively prime (and nonzero). If (x_0, y_0) is a particular solution of the equation $ax + by = c$, then any other solution of it is given by*

$$x = x_0 + bt, \quad y = y_0 - at$$

where t is an integer.

As for finding one solution, we recommend the following approach (but remember that there are others, too), based on the *Euclidean algorithm* — which is a method for finding the greatest common divisor of two (positive) integers. The Euclidean algorithm proceeds by successive divisions, as follows. Suppose we want to find the greatest common divisor of a and b, where $a > b > 0$. We first divide a by b and find the quotient q_1 and the remainder r_1; then we divide b by r_1 and find quotient q_2 and remainder r_2, and we go on like this, always dividing the previous divisor by the corresponding remainder.

We get a sequence of divisions (also called Euclidean, by the way):

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1q_2 + r_2 \\
r_1 &= r_2q_3 + r_3 \\
&\cdots\cdots \\
r_{n-2} &= r_{n-1}q_n + r_n \\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

The remainders of these divisions form a decreasing sequence $r_1 > r_2 > \cdots$ of nonnegative integers, so, at a certain moment the remainder has to be 0 (we considered this zero remainder to be r_{n+1}). We won't prove this fact here (the reader is again invited to try it as an exercise), but it is true that the greatest common divisor of a and b is precisely r_n, the last nonzero remainder. Instead, we note that starting with

$$\begin{aligned}
(a, b) = r_n = r_{n-2} - r_{n-1}q_n &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n \\
&= -r_{n-3}q_n + r_{n-2}(1 + q_{n-1}q_n)
\end{aligned}$$

and going backwards, we can find (a, b) to be a linear combination of r_{n-2} and r_{n-1}, then of r_{n-3} and r_{n-2}, and so on, until we get $(a, b) = ax + by$, for some integers x and y.

For example, we find a solution in integers for the equation $7x + 19y = 1$. Applying the Euclidean algorithm to the numbers 19 and 7 yields:

$$19 = 7 \cdot 2 + 5, \quad 7 = 5 \cdot 1 + 2, \quad 5 = 2 \cdot 2 + 1, \quad 2 = 1 \cdot 2 + 0.$$

Thus

$$\begin{aligned}
1 &= 5 - 2 \cdot 2 = 5 - (7 - 5 \cdot 1) \cdot 2 = 7 \cdot (-2) + 5 \cdot 3 \\
&= 7 \cdot (-2) + (19 - 7 \cdot 2) \cdot 3 = 7 \cdot (-8) + 19 \cdot 3,
\end{aligned}$$

and the equation has the solution $(-8, 3)$. Consequently, an arbitrary solution of $7x + 19y = 1$ is a pair of the form $(-8 + 19t, 3 - 7t)$, with integer t.

Well, it's probably the time to see the theorem working in concrete problems (some of them can very well be considered theoretical results, and can be used in solving other problems, but we will deal with them as problems, exercises, or examples).

Problem. Let a, b, and c be integers such that a and b are relatively prime and a divides bc. Prove that a divides c.

Solution. We already invited the reader to prove this result, with the help of the fundamental theorem of arithmetic. Now we use the fact that there exist integers x and y such that $ax + by = (a,b) = 1$. Thus $acx + bcy = c$, and, because ac and bc are divisible by a, it follows that c is also divisible by a.

Problem. Let a, b, c, and d be positive integers such that $ab = cd$. Prove that there are integers p, q, r, and s such that

$$a = pq, \quad b = rs, \quad c = pr, \quad d = qs.$$

Solution. If at least one of a, b, c and d is 0, the result can be easily checked. Otherwise we have $e = (a,c) \neq 0$ and $a_1 = a/e$ is relatively prime to $c_1 = c/e$, thus there exist integers x and y such that

$$a_1x + c_1y = 1.$$

Adding this equation to $a_1b - c_1d = 0$, we get

$$a_1(x + b) + c_1(y - d) = 1,$$

thus, according to the last proposition, there exists an integer t such that $x + b = x + c_1t$, and $y - d = y - a_1t$. We get $a = ea_1$, $b = c_1t$, $c = ec_1$, and $d = a_1t$, as desired.

Problem. Let m and n be positive integers, and let $d = (m,n)$. Then the common (complex) solutions of the equations $z^m = 1$ and $z^n = 1$ are the solutions of the equation $z^d = 1$. (In particular, if m and n are relatively prime, the only common solution for $z^m = 1$ and $z^n = 1$ is $z = 1$.)

Solution I. Clearly, any solution of the equation $z^d = 1$ also verifies $z^m = 1$ and $z^n = 1$ (since $z^m = (z^d)^{m/d}$, etc.). Conversely, let z be a solution of both $z^m = 1$ and $z^n = 1$. We know that there must exist $k \in \{0, 1, \ldots, m-1\}$ and $l \in \{0, 1, \ldots, n-1\}$ such that

$$z = \cos\left(\frac{2k\pi}{m}\right) + i\sin\left(\frac{2k\pi}{m}\right) = \cos\left(\frac{2l\pi}{n}\right) + i\sin\left(\frac{2l\pi}{n}\right).$$

The second equality is only possible if there exists an integer p such that

$$\frac{2k\pi}{m} = \frac{2l\pi}{n} + 2p\pi,$$

meaning that

$$kn = lm + pmn.$$

By replacing $m = dm_1$ and $n = dn_1$ (with m_1 and n_1 relatively prime integers) we get

$$kn_1 = lm_1 + pdm_1n_1.$$

Thus m_1 divides kn_1, and, because $(m_1, n_1) = 1$, actually m_1 must divide k. If we put $k = m_1q$, with integer q, we get

$$z = \cos\left(\frac{2k\pi}{m}\right) + i\sin\left(\frac{2k\pi}{m}\right) = \cos\left(\frac{2q\pi}{d}\right) + i\sin\left(\frac{2q\pi}{d}\right),$$

that is, z is a dth root of unity (a solution of the equation $z^d = 1$) — and this is precisely what we wanted to prove.

Solution II. Now let us see the main theorem in action. We only have to prove that if $z^m = 1$ and $z^n = 1$, then $z^d = 1$. Let s and t be integers such $d = ms + nt$, and let z be any complex number such that $z^m = z^n = 1$. We then have

$$z^d = z^{ms+nt} = (z^m)^s (z^n)^t = 1$$

and the proof is done. (A little bit easier, isn't it?)

The following problem does not use the theorem, but rather clarifies it under a certain aspect. Namely, we have seen that the equation $ax - by = c$ has solutions in nonnegative integers whenever a and b are positive integers and (a, b) divides c. We can ask the same question about the equation $ax + by = c$ (under the same conditions). For instance, one sees that $3x + 5y = 4$ has no solutions in nonnegative integers (although $3 \cdot (-2) + 5 \cdot 2 = 4$, or, more generally, $3(-2+5t)+5(2-3t) = 4$ for any integer t). This question can also be posed like this: what is the greatest amount that cannot be paid with coins of denominations of 3, respectively 5 monetary units? It is not hard to prove that 7 is the answer (thus the equation $3x + 5y = k$ has solutions in nonnegative integers for any $k \geq 8$, while $3x + 5y = 7$ has no such solutions). This is why such a problem is often called the *coin problem* (or the Frobenius coin problem). In general, it asks for the greatest amount that cannot be paid with coins of specified denominations of $a_1, \ldots, a_n$ monetary units, where $a_1, \ldots, a_n$ are positive relatively prime integers. In other words: what is the greatest integer k such that the equation $a_1x_1 + \cdots + a_nx_n = k$ has no solutions in nonnegative integers? No precise answer is known for the Frobenius problem with $n \geq 3$, but the case $n = 2$ was settled by Sylvester in 1884 — and this is the subject of the following problem.

Problem. Let a and b be positive relatively prime integers. Then the greatest integer that is *not* representable in the form $ax+by$, with nonnegative integers x and y is $ab - a - b$.

Solution. First we prove that $ax + by = ab - a - b$ does not have solutions in integers $x, y \geq 0$. Suppose such x and y existed. Then we would have $a(x + 1) + b(y + 1) = ab$, thus a would be a divisor of $b(y + 1)$, hence of $y + 1$ (as $(a, b) = 1$). This would lead us to $y + 1 \geq a$. Similarly, we would get $x + 1 \geq b$, but then

$$ab = a(x + 1) + b(y + 1) \geq ab + ab,$$

which is impossible.

Further we show that the equation $ax+by = k$ has solutions in nonnegative integers for any integer $k \geq ab - a - b + 1$. Indeed, one of the numbers $a \cdot 0$, $a \cdot 1, \ldots$, $a(b - 1)$ is congruent to k modulo b (they form a complete residue system modulo b). Thus there exist integers x and y with $x \in \{0, 1, \ldots, b-1\}$ (hence nonnegative) such that $ax + by = k$. But then

$$by = k - ax \geq ab - a - b + 1 - a(b-1) = -b + 1$$

is a multiple of b greater than $-b$, hence it is at least 0, implying that y is nonnegative, too, and finishing the proof.

The following problem was in many mathematical contests (for example we know it from a Romanian TST back in the year 1983), and many particular cases of it are widely known.

Problem. Let d and n be positive integers such that d and $n!$ are relatively prime. Prove that the product of n integers in arithmetic progression with common difference d is divisible by $n!$.

Solution I. We use induction on n. For $n = 1$ there is nothing to prove. Let us assume further that, for $n \geq 2$, any $n-1$ integers in arithmetic progression with common difference relatively prime to $(n-1)!$ have their product divisible by $(n-1)!$, and let us prove that if $(d, n!) = 1$ and a is any integer, then

$$a(a+d)\cdots(a+(n-1)d)$$

is divisible by $n!$. Of course, if d is relatively prime to $n!$, then it is relatively prime to $(n-1)!$, too, hence the induction hypothesis assures that

$$(a+(k+1)d)\,(a+(k+2)d)\cdots(a+(k+n-1)d)$$

is divisible by $(n-1)!$ for any integer k. That is why, if we denote

$$P_k = (a+kd)\,(a+(k+1)d)\cdots(a+(k+n-1)d)$$

(for $k \in \mathbb{Z}$), we have

$$P_{k+1} - P_k = nd\,(a+(k+1)d)\,(a+(k+2)d)\cdots(a+(k+n-1)d)$$

divisible by $n!$ for any integer k. So, it is enough to prove that P_k is divisible by $n!$ for *one* single value of k, and we can infer that this divisibility holds for *any* k. In particular, it would imply that

$$P_0 = a(a+d)\cdots(a+(n-1)d)$$

is divisible by $n!$.

Because $n!$ and d are relatively prime, there are integers s and t such that $sn! - td = 1$, implying $a + atd = asn!$. But this clearly shows that P_{at} is divisible by $n!$ (since its first factor is), and this is precisely what we needed to finish our proof.

Solution II. First note that if d and m are relatively prime integers, then among the n numbers in arithmetic progression

$$a,\ \ a+d,\ \ a+2d,\ \ \ldots,\ \ a+(n-1)d$$

there are at least $[n/m]$ that are divisible by m. Indeed, as we noticed in the proofs of some of our previous theoretical results, any block of m consecutive terms of the above sequence is a complete residue system modulo m, thus it contains a number divisible by m. Since there are at least $[n/m]$ such nonintersecting blocks, our claim is proved. (Here we denote by $[x]$ the integral part of the real number x, that is, $[x]=k$ if k is the unique integer such that $k \le x < k+1$.)

Now let p be any prime number that appears in the factorization of $n!$, and let $e_p(N)$ denote the exponent of p in the prime factorization of an integer N. Clearly, our problem is solved if we succeed to prove that

$$e_p\left(a(a+d)\cdots(a+(n-1)d)\right) \ge e_p(n!)$$

for any such p. It is well-known by a theorem of Legendre that

$$e_p(n!) = \sum_{j\ge 1}\left[\frac{n}{p^j}\right].$$

Note that this sum is not infinite; it ends with a term having the property that $p^j \le n < p^{j+1}$. Thus it remains to evaluate $e_p\left(a(a+d)\cdots(a+(n-1)d)\right)$ which we do in a similar manner as for $e_p(n!)$.

Because $p \mid n!$ and $(d,n!)=1$, we have also $(p,d)=1$, and, actually $(p^j,d)=1$ for every positive integer j. Denote by l_j the number of the terms of the sequence

$$a,\ \ a+d,\ \ a+2d,\ldots,\ \ a+(n-1)d$$

that are divisible by p^j. According to our first remark, we have

$$l_j \ge \left[\frac{n}{p^j}\right]$$

for every $j \ge 1$.

On the other hand, the exponent of p in $a(a+d)\cdots(a+(n-1)d)$ is

$$l_1 - l_2 + 2(l_2-l_3) + 3(l_3-l_4) + \cdots = l_1 + l_2 + l_3 + \cdots$$

(again, this is actually a finite sum), as, clearly, $l_j - l_{j+1}$ represents the number of terms of the sequence $a,\ \ a+d,\ \ a+2d,\ldots,\ \ a+(n-1)d$ that are divisible by p^j but not by p^{j+1} (which contribute to the exponent with a total of $j(l_j - l_{j+1})$). So, finally,

$$e_p\left(a(a+d)\cdots(a+(n-1)d)\right) = \sum_{j\geq 1} l_j \geq \sum_{j\geq 1}\left[\frac{n}{p^j}\right] = e_p(n!)$$

holds for every prime p that divides $n!$, hence the divisibility of

$$a(a+d)\cdots(a+(n-1)d)$$

by $n!$ follows.

We invite the reader to observe that, basically, we also proved the theorem of Legendre about $e_p(n!)$.

Proposed Problems

1. Prove the main theorem by inducting on n.

2. Find the solutions to the system of congruences

$$x \equiv 7 \pmod 9,\ \ x \equiv 1 \pmod{11}.$$

3. Solve the system of congruences

$$x \equiv 1 \pmod 3,\ \ x \equiv 2 \pmod 5,\ \ x \equiv 3 \pmod 7.$$

4. Let $(G, \cdot)$ be a group with identity element e, and let m and n be integers. Prove that, for $x \in G$, we have $x^m = e$ and $x^n = e$ if and only if $x^{(m,n)} = e$.

5. Let $(G, \cdot)$ be a finite group with n elements. Prove that the function $f : G \to G$ given by $f(x) = x^k$ for all $x \in G$ is bijective if and only if $(n, k) = 1$.

6. Let $(G, \cdot)$ be a group.

   a) Suppose that $x \in G$ commutes with y^m and with y^n for some $y \in G$, and for some $m, n \in \mathbb{Z}$. Prove that x commutes with $y^{(m,n)}$.

   b) For integer k, we denote by $f_k : G \to G$ the function defined by $f_k(x) = x^k$, for all $x \in G$. Assume that for some integer n the functions f_n, f_{n+1}, and f_{n+2} are homomorphisms from G into G. Prove that G is Abelian.

7. We keep the notations from the previous problem. Suppose that m and n are integers such that $(m(m-1), n(n-1)) = 2$, and such that f_m and f_n are both endomorphisms of G. Prove that G is Abelian.

8. Let $(G, \cdot)$ be a group with identity element e, and let m and n be nonzero integers. Suppose that for $x \in G$, there exist $y \in G$ and $z \in G$ such that $x = y^m = z^n$ and such that y and z commute with each other. Prove that there also exists $t \in G$ such that $x = t^{[m,n]}$ (where $[m, n]$ is the least common multiple of m and n).

9. Let m and n be positive integers. Prove that if an arithmetic progression whose first term and common difference are relatively prime nonnegative integers contains an mth power and an nth power, then it also contains an $[m, n]$th power. (An mth power is a power of an integer with exponent m.)

10. Prove that $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$ for any positive integers m and n. Can this be generalized for $(a^m - 1, a^n - 1)$, where $a \geq 2$ is a positive integer?

11. Let a and b be positive integers. Prove that the number of nonnegative integers that are *not* representable in the form $ax + by$, with x and y nonnegative integers is $(a-1)(b-1)/2$.

12. Let S be a subset of the set of positive integers, having the property that for all $x, y \in S$, we also have $x + y \in S$. Prove that S consists of all multiples of a fixed positive integer d, except for finitely many of these multiples.

13. Let $a_1, \ldots, a_n$ $(n \geq 2)$ be positive integers such that $(a_1, \ldots, a_n) = 1$. Prove that a minimal natural number $N = g(a_1, \ldots, a_n)$ exists such that any positive integer $x > N$ can be written in the form $x = x_1a_1 + \cdots + x_na_n$, with nonnegative integers $x_1, \ldots, x_n$. The minimality of N means that N itself cannot be expressed in the form $x = x_1a_1 + \cdots + x_na_n$, with nonnegative integers $x_1, \ldots, x_n$.

14. Let a, b, and c be positive integers such that $(a, b) = (a, c) = (b, c) = 1$. Prove that $2abc - ab - ac - bc$ is the greatest integer that cannot be expressed in the form $xbc + yac + zab$, where x, y, and z are nonnegative integers.

15. Let $0 < r < 1$ be a rational number. Prove that there exist positive integers $n_1 > \cdots > n_k > 1$ such that

$$r = \frac{1}{n_1} + \cdots + \frac{1}{n_k}.$$

Solutions

1. As we proved in the theoretical part, for positive and relatively prime integers a and b, there exist integers u and v such that $au - bv = 1$, hence the equation $ax + by = 1$ has solutions in integers. But the signs of a and b are not relevant in this issue. For example, if $a > 0$ and $b < 0$ are relatively prime, the same is true for a and $-b$, thus the equation $ax - by = 1$ has integer solutions, too. Since $ax - by = 1$ can also be written in the form $ax + b(-y) = 1$, the equation $ax + by = 1$ still has solutions in integers. Similarly, we proceed in any other case (and we treat the cases $a = 0$ and $b = 0$ separately).
   Now, if $(a, b) = d$, then a/d and b/d are relatively prime integers, hence the equation $(a/d)x + (b/d)y = 1$ has solutions in integers. Clearly, any such solution also satisfies $ax + by = d$ and the case $n = 2$ is thus settled.

   We assume now that the result of the theorem is true for $n - 1$, and we prove it for n. Due to the inductive hypothesis, we can find integers $u_1, \ldots, u_{n-1}$ such that

   $$a_1u_1 + \cdots + a_{n-1}u_{n-1} = (a_1, \ldots, a_{n-1}).$$

   The already proved case $n = 2$ assures the existence of some $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that

   $$(a_1, \ldots, a_{n-1})x + a_ny = ((a_1, \ldots, a_{n-1}), a_n) = (a_1, \ldots, a_n).$$

   (Use either the definition of the greatest common divisor, or its calculation with the help of factorizations, in order to prove that

   $$(a_1, \ldots, a_n) = ((a_1, \ldots, a_i), (a_{i+1}, \ldots, a_n))$$

   is true for any integers $a_1, \ldots, a_n$ and any $1 \le i \le n$.) Now it is easy to see that $x_j = u_jx$ for $1 \le j \le n - 1$ and $x_n = y$ are the components of a solution for

   $$a_1x_1 + \cdots + a_nx_n = (a_1, \ldots, a_n),$$

   which is precisely what we intended to prove.

2. We have $x \equiv 7 \pmod 9 \Leftrightarrow x = 9p + 7$ and $x \equiv 1 \pmod{11} \Leftrightarrow x = 11q + 1$ for some integers p and q. Thus we obtain the equation

   $$9p + 7 = 11q + 1 \Leftrightarrow 9p - 11q = -6.$$

   By the method described above, after finding the solution $p = 3$, $q = 3$ we must have $p = 3 + 11t$ and $q = 3 + 9t$ for integer t, which gives the solutions $x = 34 + 99t$, $t \in \mathbb{Z}$, for the initial system of congruences.

Actually, in the same way, we can prove that for $r_1, r_2, m_1, m_2 \in \mathbb{Z}$, with positive and relatively prime integers m_1 and m_2, the system of congruences

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}$$

always has solutions in integers, and all its solutions are congruent modulo $m_1 m_2$.

Indeed, we need have $x = r_1 + m_1 p = r_2 + m_2 q$, for some $p, q \in \mathbb{Z}$, thus

$$m_1 p - m_2 q = r_2 - r_1;$$

therefore, if (p_0, q_0) is a solution of this equation (since $(m_1, m_2) = 1$, such a solution does exist), we get

$$p = p_0 + m_2 t, \quad q = q_0 + m_1 t,$$

with $t \in \mathbb{Z}$. Consequently

$$x = r_1 + m_1 p_0 + m_1 m_2 t, \quad t \in \mathbb{Z}$$

are all the solutions of the system.
(We can also compute x as $x = r_2 + m_2 q_0 + m_1 m_2 t$.) Clearly, all solutions are congruent modulo $m_1 m_2$.

3. If $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$, we must have

$$x = 1 + 3p = 2 + 5q = 3 + 7r$$

for some integers p, q, and r. From $3p - 5q = 1$ we get, as before, $p = 2 + 5s$ and $q = 1 + 3s$, hence $x = 7 + 15s$, $s \in \mathbb{Z}$. Now

$$3 + 7r = 7 + 15s \Leftrightarrow 7r - 15s = 4$$

yields $r = 7 + 15t$ and $s = 3 + 7t$, $t \in \mathbb{Z}$, leading to

$$x = 52 + 105t$$

with $t \in \mathbb{Z}$.

In a similar manner we can (inductively) prove the *Chinese Remainder Theorem*: if $m_1, \ldots, m_n$ are integers such that any two of them are relatively prime, and $r_1, \ldots, r_n$ are any integers, then the system consisting of the congruences $x \equiv r_j \pmod{m_j}$, $1 \leq j \leq n$ has solutions, and all solutions are congruent modulo $m_1 \cdots m_n$. Indeed, for $n = 1$ there is nothing to prove, and the case $n = 2$ was solved at the end of the previous solution. If the theorem is true for $n - 1$, the system

$$x \equiv r_j \pmod{m_j}, \quad 1 \leq j \leq n - 1$$

has solutions of the form $x = x_0 + tm_1 \cdots m_{n-1}$, $t \in \mathbb{Z}$. So, the solutions for the system of n congruences are actually those of the system formed only by two congruences, namely

$$x \equiv x_0 \pmod{m_1 \cdots m_{n-1}} \text{ and } x \equiv r_n \pmod{m_n}.$$

But the case of two congruences is proved, thus (also keeping in mind that $m_1 \cdots m_{n-1}$ and m_n are relatively prime in the conditions of the theorem) the system has solutions, and they are all congruent modulo $(m_1 \cdots m_{n-1})m_n = m_1 \cdots m_n$.

4. This is exactly like in the problem previously solved as an example, about the common solutions of the complex equations $z^m = 1$ and $z^n = 1$. So, if we have $x^m = x^n = e$, and we consider integers u and v such that $(m, n) = um + vn$, we get

$$x^{(m,n)} = x^{um+vn} = (x^m)^u (x^n)^v = e.$$

The converse is evident. In the problem solved above the group G is specialized to $\mathbb{C}^*$ — the multiplicative group of nonzero complex numbers. Note however that the result remains true in noncommutative groups, too, since the powers of the same element always commute.

5. If k and n are not relatively prime, then they have a common prime divisor; let it be p. By Cauchy's theorem, since p divides the order n of the group, there exists in G an element g of order p, thus $g \neq e$ and $g^p = e$ (e being the identity element of G). But if $g^p = e$ and p divides k we also have $g^k = e$, hence we get $f(g) = e = f(e)$ for $g \neq e$, that is, f is not injective. Thus we proved by contraposition that if f is bijective, then n and k must be relatively prime.

Conversely, assume $(n, k) = 1$. As we know, there exist integers p and q such that $pn + qk = 1$. Remember that, by Lagrange's theorem, we have $u^n = e$ for every $u \in G$. Thus, for a given $y \in G$, we get

$$y = y^{pn+qk} = (y^n)^p (y^q)^k = (y^q)^k = f(y^q),$$

which shows that f is surjective. But, since G is a finite set, being surjective is equivalent for f (and actually for any function defined on G with values in G) to being injective (and, therefore, bijective), so, the proof is done.

6. a) It is easy to see that, for $g \in G$, the set

$$C(g) = \{z \in G \mid gz = zg\}$$

formed with the elements of G that commute with g is a subgroup of G (called the *centralizer* of g in G).
(If $h, k \in C(g)$ we have $gh = hg$ and $gk = kg$, hence

$$g(hk) = (gh)k = (hg)k = h(gk) = h(kg) = (hk)g \Rightarrow hk \in C(g).$$

Also $gh = hg$ implies $h^{-1}g = gh^{-1}$ by obvious multiplications with the inverse h^{-1} of h, thus $h^{-1} \in G$.)

Now we have $(m, n) = am + bn$ for some integers a and b and the hypothesis tells us that $y^m \in C(x)$ and $y^n \in C(x)$. In conclusion,

$$y^{(m,n)} = y^{am+bn} = (y^m)^a (y^n)^b$$

belongs to $C(x)$, too, that is, $y^{(m,n)}$ commutes with x, too.

b) We are given that $(xy)^k = x^k y^k$ is true for all $x, y \in G$, and for $k \in \{n, n+1, n+2\}$. We then have (for arbitrary, but fixed for the moment $x, y \in G$)

$$x^{n+1}y^{n+1} = (xy)^{n+1} = (xy)^n(xy) = x^n y^n xy,$$

hence, by simplifying with x^n to the left and with y to the right, we get $xy^n = y^n x$.
Similarly, from $(xy)^{n+1} = x^{n+1}y^{n+1}$ and $(xy)^{n+2} = x^{n+2}y^{n+2}$ we get $xy^{n+1} = y^{n+1}x$. Now we see that x commutes with y^n and with y^{n+1}; because n and $n+1$ are relatively prime the result from the first part applies to yield that x commutes with $y^{(n,n+1)} = y$, therefore $xy = yx$ is true for all $x, y \in G$.

Note that we can rephrase this part in the following form: if x and y are elements of a group G satisfying, for some integer n, the equalities $(xy)^k = x^k y^k$ for $k \in \{n, n+1, n+2\}$, then $xy = yx$.

7. This is a little bit more complicated. We denote by $End(G)$ the set of group endomorphisms of G (hence the hypothesis says that f_m and f_n belong to $End(G)$) and first prove the following:

   Lemma. (i) If, for some integers p and q, we have $f_p, f_{pq} \in End(G)$, then f_{p-pq} also belongs to $End(G)$. In particular, if $f_q \in End(G)$, then $f_{1-q} \in End(G)$, too.

   (ii) If $f_p \in End(G)$ and $f_{-p} \in End(G)$, then any two elements of the set $f_p(G) = \{g^p \mid g \in G\}$ commute. Moreover, every element of $f_p(G)$ is central, that is, it commutes with every element of G.

   (iii) If $f_p, f_{-p} \in End(G)$ and $f_q, f_{-q} \in End(G)$, then $f_{kp+lq} \in G$ for all $k, l \in \mathbb{Z}$. In particular, it follows that $f_{(p,q)} \in End(G)$.

(iv) If $f_p, f_q \in End(G)$, then $f_{pq} \in End(G)$.

(v) If $f_2 \in End(G)$, then G is Abelian.

Proof. (i) We have

$$\begin{aligned} x^{pq}y^{pq} &= (xy)^{pq} = ((xy)^p)^q = (x^py^p)^q = x^p(y^px^p)^{q-1}y^p \\ &= x^p((yx)^p)^{q-1}y^p = x^p(yx)^{pq-p}y^p; \end{aligned}$$

by simplifying with x^p to the left and with y^p to the right, we get

$$x^{pq-p}y^{pq-p} = (yx)^{pq-p}.$$

Now we take inverses in both sides and (using $(uv)^{-1} = v^{-1}u^{-1}$) we get

$$(yx)^{p-pq} = y^{p-pq}x^{p-pq}$$

for all x and y in G, meaning that f_{pq-p} is an endomorphism of G. The second part follows for $p = 1$, since f_1 surely is an endomorphism of G.

(ii) We know now that $(xy)^p = x^py^p$ and $(xy)^{-p} = x^{-p}y^{-p}$ for all $x, y \in G$. The second relation also gives (by taking the inverses) $(xy)^p = y^px^p$, thus we have $x^py^p = y^px^p$ and the first claim is proved. For the second, we have

$$xy^px^{-1} = (xyx^{-1})^p = x^py^px^{-p} = x^px^{-p}y^p = y^p$$

(using the fact that powers with exponent p commute with each other), therefore $xy^p = y^px$ for all x and y in G.

(iii) From the previous part we know that g^p and g^q commute with every element of G, for any $g \in G$. Thus

$$\begin{aligned} (xy)^{kp+lq} &= (xy)^{kp}(xy)^{lq} = (x^py^p)^k(x^qy^q)^l \\ &= (x^p)^k(x^q)^l(y^p)^k(y^q)^l = x^{kp+lq}y^{kp+lq}, \end{aligned}$$

after rearranging the factors x^p, x^q, y^p and y^q. The second part follows, of course, from our main theorem (that is, from the fact that (p, q) can be expressed in the form $kp + lq$, for some integers k and l).

(iv) Clearly, if $(xy)^p = x^py^p$ and $(xy)^q = x^qy^q$ for every x and y in G, then we also have

$$(xy)^{pq} = ((xy)^p)^q = (x^py^p)^q = x^{pq}y^{pq}$$

for all $x, y \in G$.

(v) This is well-known. Indeed, if we simplify with x to the left and with y to the right in $(xy)^2 = x^2y^2 \Leftrightarrow xyxy = xxyy$ we get precisely $yx = xy$.

Now we solve the problem. The hypothesis gives us f_m and f_n to be endomorphisms of G. Part (i) of the lemma says that $f_{1-m} \in End(G)$, and then, by part (iv), $f_{m-m^2} = f_{m(1-m)} \in End(G)$, too. On the other hand, $f_{m^2} = f_{m \cdot m} \in End(G)$, hence $f_{1-m^2} \in End(G)$, and, finally

$$f_{m^2-m} = f_{(1-m)-(1-m)(1+m)} \in End(G)$$

by applying part (i) again (for $p = 1-m$, $q = 1+m$, and $pq = 1-m^2$). Thus if f_m is an endomorphism, f_{m-m^2} and f_{m^2-m} are also endomorphisms of G. Similarly, because f_n is an endomorphism, the same is true for f_{n-n^2} and f_{n^2-n}. So, we can apply part (iii), for $p = m^2 - m$ and $q = n^2 - n$. It follows that $f_2 = f_{(m^2-m,n^2-n)}$ is also an endomorphism, and part (v) of the lemma justifies the commutativity of G. The proof is now complete.

This is problem D proposed by Michiel Vermeulen in *Nieuw Archief voor Wiskunde* 1/2006 with the solution of R. Bos in the same magazine 3/2006. The original statement of the problem is modified — it is more like the theorem proved in the solution. In the same mentioned solution it is also proven that if the greatest common divisor of $m(m-1)$ and $n(n-1)$ is greater than 2, then there exists a *non*commutative group G such that f_m and f_n are endomorphisms of G.

8. If $d = (m, n)$, we have $m = dm_1$ and $n = dn_1$, where m_1 and n_1 are relatively prime integers; in that case $[m, n] = mn/(m, n) = dm_1n_1$. For relatively prime m_1 and n_1, there exist integers u and v such that $um_1 + vn_1 = 1$. Note that, by hypothesis, $x = y^m = y^{dm_1}$ and $x = z^{dn_1}$. We then have

$$\begin{aligned} x = x^{um_1+vn_1} &= x^{um_1}x^{vn_1} = \left(z^{dn_1}\right)^{um_1}\left(y^{dm_1}\right)^{vn_1} \\ &= \left(z^u\right)^{dm_1n_1}\left(y^v\right)^{dm_1n_1} = \left(z^uy^v\right)^{dm_1n_1} = t^{[m,n]} \end{aligned}$$

for $t = z^uy^v \in G$. Of course, we can also have $[m, n] = -dm_1n_1$ (if m and n have opposite signs), but this is not a problem, since if it happens we can choose $t = z^{-u}y^{-v}$. Also, the result is trivially true if $m = 0$ or $n = 0$.

9. Let a and d be the first term, respectively the common difference of the progression; so a and d are relatively prime nonnegative integers. When $d = 0$, we have to prove that if a is an mth power, and also an nth power, then a is an $[m, n]$th power, too. This is clear for $a = 0$ and for $a = 1$, while if $a \geq 2$ it is a consequence of the fundamental theorem of arithmetic. Indeed, since a is an mth power, the exponents of the primes from the factorization of a must be all multiples of m; similarly, because

a is an nth power, these exponents must be multiples of n, too. But, as multiples of m and n, the exponents have to be multiples of $[m,n]$, and this means that a is an $[m,n]$th power. Also, for $d=1$ the result is obvious, since in this case the progression contains all but finitely many nonnegative integers.

Further let $d \geq 2$, and let p, q, b, and c be nonnegative integers such that $a+pd=b^m$ and $a+qd=c^n$. In the ring of residue classes $\mathbb{Z}/d\mathbb{Z}$ this means that

$$\overline{a}=\overline{b^m} \text{ and } \overline{a}=\overline{c^n}$$

(we denote by $\overline{x}$ the residue class of x modulo d).

Note that $(a,d)=1$ implies that $\overline{a}$ is invertible in $\mathbb{Z}/d\mathbb{Z}$, hence these can actually be considered as equalities in the (commutative) group $U(\mathbb{Z}/d\mathbb{Z})$ of invertible elements of $\mathbb{Z}/d\mathbb{Z}$. By the result of the previous problem, there exists $\overline{t} \in U(\mathbb{Z}/n\mathbb{Z})$ such that

$$\overline{a}=\overline{t^{[m,n]}},$$

that is

$$t^{[m,n]}=a+rd$$

for some integer r. We can choose the representative t to be a big enough integer in order to ensure that r is a positive integer, thus making the $[m,n]$th power $t^{[m,n]}$ a term of the arithmetic progression $(a+kd)_{k\geq 0}$, and finishing the proof. The reader is invited to prove that the result of this problem remains true even if we drop the condition $(a,d)=1$. (See also problem 21 in the chapter *Arithmetic and Geometric Progressions.*)

10. **Solution I.** Let

$$\begin{aligned}
m &= nq_1+r_1\\
n &= r_1q_2+r_2\\
r_1 &= r_2q_3+r_3\\
&\cdots\cdots\\
r_{k-2} &= r_{k-1}q_k+r_k\\
r_{k-1} &= r_kq_{k+1}
\end{aligned}$$

be the equations resulting from applying the Euclidean algorithm to m and n, so that $d=(m,n)=r_k$. We have

$$\begin{aligned}
2^m-1 &= 2^{r_1}(2^{nq_1}-1)+2^{r_1}-1\\
&= (2^n-1)2^{r_1}(2^{n(q_1-1)}+\cdots+2^n+1)+2^{r_1}-1
\end{aligned}$$

thus the remainder of 2^m-1 when divided by 2^n-1 is $2^{r_1}-1$. Similarly, when we divide 2^n-1 by $2^{r_1}-1$ we get the remainder $2^{r_2}-1$, and so on, meaning that the Euclidean algorithm for 2^m-1 and 2^n-1 has the form

$$\begin{aligned}
2^m-1 &= (2^n-1)Q_1+2^{r_1}-1\\
2^n-1 &= (2^{r_1}-1)Q_2+2^{r_2}-1\\
2^{r_1}-1 &= (2^{r_2}-1)Q_3+2^{r_3}-1\\
&\cdots\cdots\\
2^{r_{k-2}}-1 &= (2^{r_{k-1}}-1)Q_k+2^{r_k}-1\\
2^{r_{k-1}}-1 &= (2^{r_k}-1)Q_{k+1}
\end{aligned}$$

for some integers $Q_1,\dots,Q_{k+1}$ (that do not matter for our proof). Thus the greatest common divisor of 2^m-1 and 2^n-1 is $2^{r_k}-1=2^{(m,n)}-1$, as claimed.

Solution II. As in the first solution, we use the fact that if x and y are positive integers such that x is divisible by y, then 2^x-1 is divisible by 2^y-1. More precisely, if $x=yz$, we have

$$2^x-1=(2^y)^z-1=(2^y-1)(2^{y(z-1)}+2^{y(z-2)}+\cdots+2^y+1).$$

Thus, if $d=(m,n)$, because $d\mid m$ and $d\mid n$, we also have that 2^d-1 divides both 2^m-1 and 2^n-1. Further, there exist positive integers s and t such that $sm-tn=d$, hence

$$\begin{aligned}
(2^m-1)(2^{m(s-1)}+2^{m(s-2)}+\cdots+2^m+1) &= 2^{sm}-1=2^d(2^{tn}-1)+2^d-1\\
&= (2^n-1)2^d(2^{n(t-1)}+2^{n(t-2)}+\cdots+2^n+1)+2^d-1.
\end{aligned}$$

Now, the equality

$$\begin{aligned}
&(2^m-1)(2^{m(s-1)}+2^{m(s-2)}+\cdots+2^m+1)\\
&= (2^n-1)2^d(2^{n(t-1)}+2^{n(t-2)}+\cdots+2^n+1)+2^d-1.
\end{aligned}$$

shows that any divisor of 2^m-1 and 2^n-1 also divides 2^d-1, and we can conclude that $2^d-1=(2^m-1,2^n-1)$.

One sees that nothing changes in either of the above solutions if we replace 2 by some $a\geq 2$. Thus, for any positive integers $a\geq 2$, m, and n we have $(a^m-1,a^n-1)=a^{(m,n)}-1$.

11. We say that n is representable if there are nonnegative integers x and y such that $n=ax+by$ (and non-representable if such x and y do not

exist). As we have seen, $N = ab - a - b$ is the greatest non-representable integer. So the numbers that are not representable are among $0, 1, \dots, N$. Let $n \in \{0, 1, \dots, N\}$; we see immediately that n and $N - n$ cannot be both representable, since if they were, their sum N would also be representable — but we know that it isn't.

Now suppose n is *not* representable. Nevertheless, there must be some $y \in \{0, 1, \dots, a-1\}$ such that $n - by$ is a multiple of a, say $n - by = ax$ with integer x. Because $n = ax + by$, $y \geq 0$, and n is non-representable, we necessarily have $x \leq -1$, or $x + 1 \leq 0$. So,

$$N - n = ab - a - b - ax - by = -(x+1)a + (a - 1 - y)b$$

is representable, as $-(x+1) \geq 0$ and $a - 1 - y \geq 0$.

In conclusion, for any $n \in \{0, 1, \dots, N\}$, precisely one of n and $N - n$ is representable. This shows that the number of non-representable integers is half the cardinality of $\{0, 1, \dots, N\}$, that is,

$$(N+1)/2 = (a-1)(b-1)/2.$$

12. Clearly, S must be infinite, since all multiples nx, $n \in \mathbb{N}^*$ of an element $x \in S$ must be in S, too. Actually, a standard inductive argument shows that, if $x_1, \dots, x_p \in S$, and $n_1, \dots, n_p \in \mathbb{N}^*$, then $n_1x_1 + \cdots + n_px_p$ also belongs to S. Since for every element of S all its multiples are in S, the set $M = \{m \in \mathbb{N}^* \mid \exists\ k_0 \in \mathbb{N}^* \text{ such that } \ km \in S,\ \forall\ k \geq k_0\}$ is nonempty. Being a subset of the set of positive integers, it has a minimum element, let it be d. So, for d we have $kd \in S$ for all positive integers $k \geq k_0$ (for a certain k_0), and if some $d_1 \in \mathbb{N}^*$ also has the property that $kd_1 \in S$ for all $k \geq k_1$, then $d_1 \geq d$. (Note that d does *not* necessarily belong to S.)

    Now let x be an arbitrary element of S, and let $\delta = (d, x)$ be the greatest common divisor of d and x. Also, let $q \geq k_0$ be such that $(q, x) = 1$ (we can always choose such q, for example of the form $1 + tx$, for sufficiently big t). We thus have $qd \in S$, and $(qd, x) = \delta$, since q and x have no common factors (other than 1). Because qd/δ and x/δ are relatively prime we know (by the Frobenius problem for two numbers) that every big enough positive integer can be expressed as $n_1(qd/\delta) + n_2(x/\delta)$, with n_1 and n_2 nonnegative integers. It follows that all but finitely many multiples of δ can be expressed as $n_1(qd) + n_2x$, where $n_1, n_2 \in \mathbb{N}$, hence, as noticed in the beginning (and because qd and x are in S), they belong to S. This means that δ is a member of M and, consequently, $\delta \geq d$. On the other hand, δ is a divisor of d, therefore $\delta \leq d$. So, finally, we get $\delta = d$, thus we have $d = (d, x)$, that is, d is a divisor of x — and this is for any $x \in S$.

Summarizing, we see that we obtained

$$\{kd \mid k \geq k_0\} \subseteq S \subseteq \{kd \mid k \in \mathbb{N}^*\},$$

which is exactly what we intended to prove: S consists of all multiples of d, possibly with finitely many exceptions. As we said before, d does not necessarily belong to S; for example, S can consist of

$$6, 10, 12, 16, 18, 20, 22, 24, \ldots$$

(here $d = 2$ and S contains all multiples $2k$ of 2, with $k \geq 8$, and also its multiples $6, 10, 12$). If, however, $d \in S$, then S is, of course, formed with precisely all positive multiples of d.

The example above also shows that S is not necessarily a set of the form $\{kd \mid k \geq k_0\}$, but rather the union of such a set with a finite set of multiples of d smaller than $k_0 d$.

13. The number $g(a_1, \ldots, a_n)$ is called the *Frobenius number* of the set $\{a_1, \ldots, a_n\}$, and its existence was proved for $n = 2$ (as we have seen, at the end of nineteenth century Sylvester showed that $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$; by the way, the fact that in this case the number of positive integers non-representable as $x_1 a_1 + x_2 a_2$, with $x_1, x_2 \geq 0$ is $(a_1 - 1)(a_2 - 1)/2$ — see problem 11 — was also proved by Sylvester). For $n > 2$ there are no formulae for $g(a_1, \ldots, a_n)$, although various (more or less efficient) algorithms for computing it are known. However, to prove that $g(a_1, \ldots, a_n)$ exists is a much easier task — achievable, for example, by an inductive approach.

Assume thus that $g(b_1, \ldots, b_{n-1})$ exists for any positive relatively prime integers $b_1, \ldots, b_{n-1}$, and let $a_1, \ldots, a_n$ be positive relatively prime integers. Let $d = (a_1, \ldots, a_{n-1})$, so that $(a_1/d, \ldots, a_{n-1}/d) = 1$, and $(d, a_n) = 1$, too. Let x be a positive integer such that

$$x > dg\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}\right) + (d-1)a_n.$$

Because d and a_n are relatively prime, one of the numbers x, $x - a_n, \ldots$, $x - (d-1)a_n$ is a multiple of d, so there exist integers y and $x_n \in \{0, 1, \ldots, d-1\}$ such that

$$x = yd + x_n a_n.$$

Now we have

$$yd = x - x_n a_n \geq x - (d-1)a_n > dg\left(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}\right),$$

hence there exist nonnegative integers $x_1, \ldots, x_{n-1}$ such that

$$y = x_1\frac{a_1}{d} + \cdots + x_{n-1}\frac{a_{n-1}}{d} \Leftrightarrow yd = x_1a_1 + \cdots + x_{n-1}a_{n-1};$$

therefore, any $x > dg(a_1/d, \ldots, a_{n-1}/d) + (d-1)a_n$ can be represented as $x_1a_1 + \cdots + x_na_n$, where $x_1, \ldots, x_n$ are nonnegative integers — showing that $g(a_1, \ldots, a_n)$ exists and is at most $dg(a_1/d, \ldots, a_{n-1}/d) + (d-1)a_n$.

14. Suppose $2abc - ab - ac - bc = xbc + yac + zab$, with integers $x, y, z \geq 0$. Since $a(2bc - b - c - yc - zb) = bc(x+1)$ and a is relatively prime to b and c (thus to bc), we have that a divides $x + 1$, hence $x + 1 \geq a$; similarly, $y + 1 \geq b$ and $z + 1 \geq c$, therefore

$$2abc = (x+1)bc + (y+1)ac + (z+1)ab \geq 3abc,$$

which is impossible.

Now let w be an integer greater than $2abc - ab - ac - bc$. Because

$$c(a-1)(b-1) \geq 0 \Leftrightarrow abc - ac - bc + c \geq 0,$$

we also have

$$2abc - ab - ac - bc \geq abc - ab - c,$$

hence $w > (ab)c - ab - c$. Further, ab and c are relatively prime, thus, by the Frobenius problem for the numbers ab and c, there exist nonnegative integers t and z such that

$$w = tc + zab.$$

Moreover, we know that in this representation z can be chosen to be at most $c - 1$ (see the proof). Then

$$tc = w - zab > 2abc - ab - ac - bc - (c-1)ab = abc - ac - bc,$$

that is, $t > ab - a - b$. Also, a and b are relatively prime, hence (applying the result of the Frobenius problem once again, for a and b) there are nonnegative integers x and y such that $t = xb + ya$. It follows that

$$w = tc + zab = (xb + ya)c + zab = xbc + yac + zab,$$

where x, y, and z are nonnegative integers, and the proof is complete.

This was problem 3 from the first day of the twenty-fourth International Mathematical Olympiad, held in 1983, in France.

15. Let $r = a/b$ with positive integers a and b such that $(a, b) = 1$. If $a = 1$, then we are done, so we assume $a > 1$. Then we can find positive integers x_1 and y_1 such that $ay_1 - bx_1 = 1$, or

$$\frac{a}{b} - \frac{x_1}{y_1} = \frac{1}{by_1}.$$

Moreover, we know that we can choose x_1 to be less than a, and y_1 less than b. Since x_1 and y_1 are relatively prime, there exist positive relatively prime integers x_2 and y_2 such that $x_1 > x_2$, $y_1 > y_2$, and

$$x_1y_2 - y_1x_2 = 1 \Leftrightarrow \frac{x_1}{y_1} - \frac{x_2}{y_2} = \frac{1}{y_1y_2}.$$

Further, since $(x_2, y_2) = 1$, let $x_3 < x_2$ and $y_3 < y_2$ be such that

$$x_2y_3 - y_2x_3 = 1 \Leftrightarrow \frac{x_2}{y_2} - \frac{x_3}{y_3} = \frac{1}{y_2y_3}.$$

In general, suppose we found

$$a = x_0 > x_1 > \cdots > x_{n-1} \quad \text{and} \quad b = y_0 > y_1 > \cdots > y_{n-1}$$

such that $(x_j, y_j) = 1$, $0 \le j \le n-1$, and

$$\frac{x_j}{y_j} - \frac{x_{j+1}}{y_{j+1}} = \frac{1}{y_jy_{j+1}}, \quad 0 \le j \le n-2.$$

Then there are positive relatively prime integers x_n and y_n such that $x_{n-1} > x_n$, $y_{n-1} > y_n$, and

$$x_{n-1}y_n - y_{n-1}x_n = 1 \Leftrightarrow \frac{x_{n-1}}{y_{n-1}} - \frac{x_n}{y_n} = \frac{1}{y_{n-1}y_n}.$$

Of course, this procedure cannot go on indefinitely.
Because $x_0 > x_1 > \cdots$ is a decreasing sequence of positive integers, there must be some s such that $x_s = 1$. The same happens for the decreasing sequence $y_0 > y_1 > \cdots$, but note that all fractions x_j/y_j are less than 1, since they also form a decreasing sequence, with the first term less than 1:

$$1 > \frac{a}{b} = \frac{x_0}{y_0} > \frac{x_1}{y_1} > \cdots$$

(just observe that the difference between each fraction and the next one is positive). So, we always have $x_j < y_j$, hence when we come to $x_s = 1$, we still have $y_s > 1$.

Now, by adding all equalities

$$\frac{x_j}{y_j} - \frac{x_{j+1}}{y_{j+1}} = \frac{1}{y_j y_{j+1}}, \quad 0 \le j \le s-1,$$

we get

$$\frac{a}{b} = \frac{1}{y_0 y_1} + \cdots + \frac{1}{y_{s-1} y_s} + \frac{x_s}{y_s} = \frac{1}{y_0 y_1} + \cdots + \frac{1}{y_{s-1} y_s} + \frac{1}{y_s}.$$

This is the required expression for a/b, since

$$y_0 y_1 > y_1 y_2 > \cdots > y_{s-1} y_s > y_s > 1.$$

For example, if we start with $r = 7/15$, we first have $7 \cdot 13 - 15 \cdot 6 = 1$, hence

$$\frac{7}{15} - \frac{6}{13} = \frac{1}{15 \cdot 13}$$

Continuing the procedure we get

$$\frac{7}{15} = \frac{1}{15 \cdot 13} + \frac{1}{13 \cdot 11} + \frac{1}{11 \cdot 9} + \frac{1}{9 \cdot 7} + \frac{1}{7 \cdot 5} + \frac{1}{5 \cdot 3} + \frac{1}{3}$$

which was actually easy to guess for someone who knew the identity

$$\sum_{j=1}^{n} \frac{1}{(2j-1)(2j+1)} = \frac{n}{2n+1}.$$

Note that we can apply the method described above to fractions greater than 1, too. For instance, by the same procedure we get

$$\frac{22}{17} = \frac{1}{17 \cdot 7} + \frac{1}{7 \cdot 4} + \frac{1}{4 \cdot 1} + 1,$$

thus the xs and ys arrive to be 1 at the same moment. Try to see what happens if you apply the same procedure to other rational numbers greater than 1!

The expression of a positive rational number as the sum of distinct fractions with numerator 1 and denominator greater than 1 is known as the Egyptian fraction decomposition of the initial number, and it exists for any positive rational number (as the name indicates, the Egyptians used such decompositions to work with fractions). We only proved the existence of such an expression for rational numbers less than 1. Try to prove it in the general case! (To begin, try to write 22/17 in this form.) Of course, such an expression of a rational number is far from being unique. It is enough to notice that an equality like

$$\frac{1}{a}=\frac{1}{a+1}+\frac{1}{a(a+1)}$$

allows us to get more and more expressions of the same form.
For instance

$$1=\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=\frac{1}{2}+\frac{1}{3}+\frac{1}{7}+\frac{1}{42}=\frac{1}{2}+\frac{1}{3}+\frac{1}{7}+\frac{1}{43}+\frac{1}{1806},$$

and so on. We also invite the reader to find other approaches for proving the existence (and non-uniqueness) of the Egyptian fractions decomposition of a given positive rational number (there are plenty of them).

Chapter 3

Squares

It is perhaps useless to say that the perfect squares are those positive integers n which can be expressed as $n = k^2$ where k is an integer. It also might seem useless to ask why they are called squares because everybody knows what "squaring" means. However, before the algebraic operation of squaring was even defined, the "square" was only a geometrical figure. It is not hard to see that n points can be neatly arranged in a figure resembling a square only when n is a perfect square.

This might seem like pure coincidence as well, but the reader probably knows that the numbers n which can be expressed as

$$n = \frac{k(k+1)}{2}$$

with $k \in \mathbb{Z}$ are called *triangular numbers*, while the numbers n which can be expressed as

$$n = \frac{k(3k+1)}{2}$$

with $k \in \mathbb{Z}$ are called *pentagonal numbers* for the same reason. By the way, pentagonal numbers, which seem like the perfect candidates for those kind of numbers without any important property are in fact extremely important in the theory of partitions. Euler discovered an important recurrence for the sequence $p(n)$ involving pentagonal numbers. We recall that the function p counts the number of ways in which a positive integer can be expressed as a sum of positive integers, without taking order into account.

The quadratic world is vast and a chapter named *Squares* should be longer than a book. But we only want to make a brief presentation of the most important facts from number theory about squares and related concepts and problems.

Quadratic Residues. There are many simple properties of the sequence

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, \ldots$$

of the perfect squares which pop up immediately even at first glance. One of the most common is the fact that the last digit of the perfect squares repeats periodically. This obviously follows from the fact that

$$n^2 \equiv (n+10)^2 \pmod{10}.$$

It is a trick frequently used by many students that the last digit of a perfect square belongs to the sequence $0, 1, 4, 5, 6, 9$. But what is in fact this last digit? Of course, the remainder $n^2 \pmod{10}$. And what is so special about this number 10? Despite the fact that we have chosen it to be the number of digits we use, nothing. So, we should try to extend this idea to other numbers besides 10.

Before taking the big step to the general case, the reader should know about some very simple, but not less important particular small cases. Every integer is either of the form $3k$ or of the form $3k \pm 1$, for some integer k. Obviously, we have

$$(3k)^2 = 9k^2 \equiv 0 \pmod 3$$

and

$$(3k \pm 1)^2 = 9k^2 \pm 6k + 1 \equiv 1 \pmod 3,$$

so the only possible remainders are 0 and 1. Similarly, every integer is either even, or odd, so

$$(2k)^2 = 4k^2 \equiv 0 \pmod 4$$

and

$$(2k+1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4,$$

so, in the case of division by 4, the only possible remainders are again only 0 and 1.

Let us consider an arbitrary odd prime number p. The number $r \in \mathbb{Z}$ is said to be a *quadratic residue modulo* p if and only if there is a positive integer k such that

$$k^2 \equiv r \pmod p.$$

Otherwise, it is called a *quadratic nonresidue modulo* p. It is apparent that all perfect squares are always quadratic residues. In particular, so are 0 and 1. For a fixed p, we define the function

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{-1, 0, 1\}$$

called the *Legendre symbol.* By definition, $\left(\frac{x}{p}\right)$ is equal to 0 if $p \mid x$, 1 if p does not divide x but x is a quadratic residue modulo p, and -1 if x is a quadratic nonresidue mod p. The following are the most important and most useful properties of the Legendre symbol.

1.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p},\ \forall a \in \mathbb{Z}.$$

2.

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),\ \forall a, b \in \mathbb{Z}.$$

3. *The Quadratic Reciprocity Law:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

where p and q are odd primes.

4.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

We will not prove these properties, but, at least, we will try to make the reader familiar with the concepts required for their proofs. The set

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$$

of nonzero residues mod p has the property that there is an element $g \in \mathbb{Z}_p^*$ such that

$$\mathbb{Z}_p^* = \left\{1, g, g^2, \ldots, g^{p-2}\right\}.$$

Of course, we are working in $\mathbb{Z}_p$ which means that we consider $a = b$ whenever $p \mid a - b$. Such elements are called *generators* and the number of them is $\phi(p-1)$, where ϕ is Euler's totient function. This function counts the number of positive integers not exceeding n which are relatively prime to it. In this case, the set of quadratic residues from $\mathbb{Z}_p^*$ is

$$\left\{1, g^2, g^4, \ldots, g^{p-3}\right\},$$

while the set of quadratic nonresidues mod p from $\mathbb{Z}_p^*$ is

$$\left\{g, g^3, g^5, \ldots, g^{p-2}\right\}.$$

Now we can see that properties 1 and 2 are immediate. Property 3 is harder to prove (although there are 6 proofs by Gauss!) and property 4 requires some work. An important consequence that we haven't mentioned so far is the fact that the number of quadratic residues mod p, as well as the number of quadratic nonresidues mod p is $\frac{p-1}{2}$ for every odd prime p.

Pell's Equation. In general, a diophantine equation of the form

$$ax^2 - by^2 = 1$$

where a and b are fixed integer parameters is said to be *Pell-type equation.* This kind of equation does not always have a solution, but in the case it has at least one, then there are infinitely many other solutions. The simplest and most important is called in fact *Pell's equation*:

$$x^2 - dy^2 = 1,$$

where $d > 0$ is not a perfect square. An important theorem in number theory states that this equation is always solvable and has infinitely many solutions.

Again, we skip the proof, but we mention that the most important step in solving this equation is finding the *fundamental* solution (x_0, y_0), i.e, the smallest solution different from $(1, 0)$. All other solutions (x_n, y_n) are given by

$$\left(x_0 + y_0\sqrt{d}\right)^n = x_n + y_n\sqrt{d}.$$

A similar yet still very important Pell-type equation is the *negative Pell equation*:

$$x^2 - dy^2 = -1.$$

This equation does not always have solutions. Of course, it is a Pell-type equation because it is the same thing as

$$dy^2 - x^2 = 1$$

and hence, in the case it has at least one solution, there are infinitely many others. A very useful property is the fact that the negative Pell equation

$$x^2 - py^2 = -1$$

where $p \equiv 1 \pmod 4$ is a prime always has a solution.

Representations with sums of squares. There are a few natural questions that arise about numbers which can be expressed as sum of squares. Which numbers can be expressed as the sum of two squares? Which numbers can be expressed as the sum of three squares? Can we say for sure that every positive integer is the sum of at most x squares? Let us state three important results from number theory which answer these questions.

1. A positive integer can be expressed as the sum of two squares if and only if every prime number of the form $4k + 3$ in its prime factorization has an even exponent (maybe 0).

2. A positive integer can be expressed as the sum of three squares if and only if it is *not* of the form $4^k\,(8l + 7)$, with natural numbers k and l (Gauss did this one, too).

3. *The four-square theorem.* Every nonnegative integer is the sum of (at most) four squares. (See the last problem from the first chapter. This is also called Lagrange's theorem.)

The proofs are entirely elementary (or at least one proof for each statement since there are also non-elementary proofs) but quite hard. We say only a few things about the first since it occurs in lots of situations. A simple, but important thing is that if $p \equiv 3 \pmod 4$ is a prime number and $p \mid a^2 + b^2$, then $p \mid a$ and $p \mid b$. It is easy to see that this implies the "only if" part of the first statement. But why is it true? If p divides either a or b, then it also divides the other, so we only have to prove that the case when p does not divide both a and b is impossible. Since $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd. We have

$$a^2 \equiv -b^2 \pmod p \Rightarrow \left(a^2\right)^{\frac{p-1}{2}} \equiv \left(-b^2\right)^{\frac{p-1}{2}} \pmod p \Rightarrow a^{p-1} \equiv -b^{p-1} \pmod p$$

which is false since we know by Fermat's little theorem that

$$a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$$

and the proof is complete. The "if" part is much harder. Still, it can be reduced a lot by using the well-known *Diophantus-Brahmagupta-Fibonacci* identity (a particular case of the *Lagrange identity*):

$$\left(a^2 + b^2\right)\left(x^2 + y^2\right) = (ax + by)^2 + (ay - bx)^2.$$

Now we can see that it is enough to prove that every prime number

$$p \equiv 1 \pmod 4$$

can be expressed as the sum of two perfect squares, which is not so easy. The shortest proof requires some knowledge of the ring $\mathbb{Z}[i]$ — but we present an elementary proof in the first chapter.

Let us see now some applications of the previous results. First, a warm-up combining inequalities and number theory.

Problem. Prove that $2^{2n+2} + 2^{m+2} + 1$, where $0 \le m \le 2n$ are integers, is a perfect square if and only if $m = n$.

Solution. Clearly, if $m = n$ then

$$2^{2n+2} + 2^{m+2} + 1 = (2^{n+1} + 1)^2.$$

Suppose now that $2^{2n+2} + 2^{m+2} + 1 = x^2$. If $m < n$, then

$$(2^{n+1})^2 < 2^{2n+2} + 2^{m+2} + 1 < (2^{n+1} + 1)^2,$$

thus

$$2^{n+1} < x < 2^{n+1} + 1,$$

which is impossible. So, suppose that $m > n$ and $m \le 2n$. Clearly, x is odd and because $2^{m+2} \mid (x-1)(x+1)$, one of the numbers $x - 1$ and $x + 1$ is a multiple of 2^{m+1}, thus, because $m \ge 2n - m + 2$, it follows that

$$2^{m+1} - 2 \ge 2^{2n-m+3} - 2 = 4 \cdot 2^{2n-m+1} - 2 > 2^{2n-m+1} + 2,$$

which in turn implies that

$$(x-1)(x+1) \geq 2^{m+1}(2^{m+1}-2) > 2^{m+2}(2^{2n-m}+1),$$

which contradicts $(x-1)(x+1) = 2^{m+2}(2^{2n-m}+1)$. This shows that $m = n$.

We continue with a beautiful application of the four-square theorem and a special case of the famous Waring problem.

Problem. Prove that for any positive integer n, the equation

$$n = x_1^4 + x_2^4 + \ldots + x_{53}^4$$

has solutions in integers.

Solution. Let us observe that

$$(a-b)^4 + (a+b)^4 = 2(a^4 + b^4 + 6a^2b^2).$$

This implies the identity

$$\sum_{1 \leq i < j \leq 4} (a_i - a_j)^4 + (a_i + a_j)^4 = 6\left(\sum_{i=1}^{4} a_i^2\right)^2.$$

Thus, using the four-square theorem, we deduce that for all $n \geq 0$, $6n^2$ is the sum of 12 fourth-powers. Now, using again the four-squares theorem, we conclude that any multiple of 6 is the sum of 48 fourth-powers. It remains to observe that any positive integer is of the form $6k + r$ with $0 \leq r \leq 5$, and any $0 \leq r \leq 5$ is the sum of at most 5 fourth powers.

Problem. Prove that the set $\{1^2, 2^2, \ldots, n^2\}$ of the first n nonzero squares can be partitioned into three subsets having the same sum of elements if and only if n is of one of the forms $9k$, $9k-1$, or $9k-5$, with $k \geq 2$ a positive integer.

Solution. Suppose first that a partition as required by the problem exists; then, of course, the sum of elements in each class of the partition must be

$$(1^2 + 2^2 + \cdots + n^2)/3 = n(n+1)(2n+1)/18,$$

hence $n(n+1)(2n+1)$ must be divisible by 9. As no two of the three factors n, $n+1$, and $2n+1$ can be simultaneously divisible by 3, it follows that one of them must be divisible by 9. That is, one of n, $n+1$, and $2n+1$ is divisible by 9, meaning that n has one of the forms $9k$, $9k-1$, $9k-5$, with k a positive integer. To prove that k is at least 2, we need to show that none of the sets

$$\{1^2, 2^2, \ldots, 9^2\}, \quad \{1^2, 2^2, \ldots, 8^2\}, \quad \{1^2, 2^2, 3^2, 4^2\}$$

can be partitioned as requested by the problem. This is obvious for the third set because if this was possible the sum in each subset would be 10 — but one subset must contain $4^2 = 16$. If the set $\{1^2, 2^2, \ldots, 9^2\}$ could be partitioned, the sum of the elements in each subset would be 95. As one of the classes of the partition must contain 64, in that class, there would be a few squares adding to 31 — but it's easy to see that this cannot happen. The same reasoning shows that the second set cannot be partitioned as required (the sum of elements in each subset has to be 68 and one subset must contain 49).

Now, for the converse, let $P(n)$ be the statement of the problem, asserting that the set of the first n nonzero squares can be partitioned into three subsets with the same sum of elements. The partition

$$\begin{aligned}&\{(n+1)^2, (n+2)^2, \ldots, (n+18)^2\}\\ =\ &\{(n+1)^2, (n+6)^2, (n+9)^2, (n+10)^2, (n+14)^2, (n+17)^2\}\\ \cup\ &\{(n+2)^2, (n+5)^2, (n+7)^2, (n+12)^2, (n+15)^2, (n+16)^2\}\\ \cup\ &\{(n+3)^2, (n+4)^2, (n+8)^2, (n+11)^2, (n+13)^2, (n+18)^2\}\end{aligned}$$

shows that each set of 18 consecutive squares can be partitioned into three subsets with the same sum of elements, therefore the implication $P(n) \Rightarrow P(n+18)$ follows easily. In order to finish the proof, we only need to prove that $P(13), P(17), P(18), P(22), P(26), P(27)$ are true. And they are indeed, because we can exhibit the partitions:

$$\begin{aligned}\{1^2, \ldots, 13^2\} &= \{1^2, 3^2, 5^2, 6^2, 9^2, 11^2\} \cup \{2^2, 10^2, 13^2\} \cup \{4^2, 7^2, 8^2, 12^2\};\\ \{1^2, \ldots, 17^2\} &= \{1^2, 2^2, 13^2, 14^2, 15^2\} \cup \{3^2, 4^2, 5^2, 16^2, 17^2\}\\ &\quad \cup \{6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2\};\\ \{1^2, \ldots, 18^2\} &= \{1^2, 6^2, 9^2, 10^2, 14^2, 17^2\} \cup \{2^2, 5^2, 7^2, 12^2, 15^2, 16^2\}\\ &\quad \cup \{3^2, 4^2, 8^2, 11^2, 13^2, 18^2\};\\ \{1^2, \ldots, 22^2\} &= \{1^2, 3^2, 6^2, 13^2, 17^2, 19^2, 20^2\}\\ &\quad \cup \{2^2, 5^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 14^2, 15^2, 16^2\}\\ &\quad \cup \{4^2, 18^2, 21^2, 22^2\};\\ \{1^2, \ldots, 26^2\} &= \{1^2, 4^2, 14^2, 20^2, 21^2, 22^2, 23^2\}\\ &\quad \cup \{2^2, 5^2, 6^2, 7^2, 8^2, 11^2, 12^2, 13^2, 15^2, 16^2, 17^2, 18^2, 19^2\}\\ &\quad \cup \{3^2, 9^2, 10^2, 24^2, 25^2, 26^2\};\\ \{1^2, \ldots, 27^2\} &= \{1^2, 2^2, 3^2, 4^2, 5^2, 15^2, 25^2, 26^2, 27^2\}\\ &\quad \cup \{6^2, 7^2, 9^2, 11^2, 12^2, 13^2, 16^2, 17^2, 18^2, 20^2, 21^2\}\\ &\quad \cup \{8^2, 10^2, 14^2, 19^2, 22^2, 23^2, 24^2\}.\end{aligned}$$

And thus we are done.
The following problem is more challenging than the solution seems to indicate.

Problem. Let a, b be integers such that $a \cdot 2^n + b$ is a perfect square for all positive integers n. Prove that $a = 0$.

Solution. Clearly, $a \geq 0$, otherwise $a \cdot 2^n + b$ becomes negative for large n. Suppose that $a > 0$ and let x_n be a nonnegative integer such that $x_n^2 = a \cdot 2^n + b$. Observe that

$$\begin{aligned} |x_{n+2} - 2x_n| &= |\sqrt{4a \cdot 2^n + b} - \sqrt{4a \cdot 2^n + 4b}| \\ &= \frac{3|b|}{\sqrt{4a \cdot 2^n + b} + \sqrt{4a \cdot 2^n + 4b}} < 1 \end{aligned}$$

for large enough n. Thus there is an n such that $x_{n+2} = 2x_n$, which implies $b = 4b$, thus $b = 0$. But for $a > 0$, $a \cdot 2^n$ cannot be a square for all n (just look at the exponent of 2 in its factorization) — which is a contradiction, and $a = 0$ remains the only possibility (with b being a square).

We end this theoretical part with two more difficult problems.

Problem. Prove that for all $n \geq 1$, there are n consecutive positive integers, none of which can be written as $a^2 + 2b^2$ for $a, b \in \mathbb{Z}$.

Solution. Using Dirichlet's theorem, we can find an infinite sequence $(p_n)_{n \geq 1}$ of prime numbers of the form $8k + 7$. From the Chinese Remainder Theorem, there exists a positive integer x such that $x + i \equiv p_i \pmod{p_i^2}$ for $1 \leq i \leq n$. We claim that none of the numbers $x + 1, x + 2, \ldots, x + n$ can be written as $a^2 + 2b^2$ for $a, b \in \mathbb{Z}$. Suppose that $1 \leq i \leq n$ and $x + i = a^2 + 2b^2$. Then $p_i \mid a^2 + 2b^2$. If $p_i \pmod{b}$, then $-2 \equiv (ab^{-1})^2 \pmod{p_i}$, where b^{-1} is the inverse of b modulo p_i. Thus $\left(-\frac{2}{p_i}\right) = 1$, which implies

$$(-1)^{\frac{p_i-1}{2} + \frac{p_i^2-1}{8}} = 1,$$

that is $\frac{p_i - 1}{2} + \frac{p_i^2 - 1}{8}$ is even, which contradicts the fact that $p_i \equiv 7 \pmod{8}$. Thus $p_i \mid b$ and so $p_i \mid a$. But then $p_i^2 \mid x + i$, which is absurd.

Finally, a very difficult example of use of the Pell equation, created by Gabriel Dospinescu.

Problem. Is there a polynomial f in two variables with integer coefficients such that

$$\{f(m,n) \mid m, n \in \mathbb{Z}\} \cap \{1, 2, 3, \ldots\} = \{x_n^{2007} \mid n \geq 1\},$$

where $x_n = \dfrac{(1 + \sqrt{2})^n + (1 - \sqrt{2})^n}{2}$?

Solution. The answer is positive. Let us consider

$$f(X, Y) = X^{2007}(2 - (X^2 - 2Y^2)^2).$$

If $m, n \in \mathbb{Z}$, then we clearly have

$$f(m,n) > 0 \Leftrightarrow 2 > (m^2 - 2n^2)^2 \Leftrightarrow |m^2 - 2n^2| = 1.$$

It is not difficult to show that the solutions of the last equation are given by

$$m_k - n_k\sqrt{2} = (1 - \sqrt{2})^k,$$

which implies that

$$\{f(m,n) \mid m,n \in \mathbb{Z}\} \cap \{1,2,\ldots\} = \{f(m_k,n_k) \mid k \geq 1\}$$
$$= \{m_k^{2007} \mid k \geq 1\} = \{x_k^{2007} \mid k \geq 1\}.$$

Proposed Problems

1. Prove that the successor of the product of four positive integers is a perfect square.

2. In what case are $m^2 + n$ and $n^2 + m$, $m, n \geq 1$ both squares?

3. A student writes a 9-digit number in which each digit from 1 to 9 occurs exactly once. Prove that the student can erase at most 7 digits such that the number obtained is a perfect square.

4. Can it happen that a number of the form $111\ldots111$ is the sum of two squares?

5. Prove that there are infinitely many pairs of perfect squares which can be written using the same digits.

6. A student writes all numbers $1^2, 2^2, \ldots, 99^2$ in a line on a blackboard. Is the big number obtained a perfect square or not?

7. Prove that a number is a perfect square iff the number of its positive divisors is odd.

8. If n is a positive integer and $d(n)$ is the number of positive divisors of n, prove that $n^{d(n)}$ is a perfect square.

9. Which positive integers can be expressed as the difference of two perfect squares?

10. Prove that if two positive integers can be expressed as the difference of two perfect squares, then their product also has this property.

11. Prove that every positive integer can be expressed as

$$\pm 1^2 \pm 2^2 \pm \ldots \pm n^2$$

for some n.

12. Prove that there are infinitely many n such that

$$n^2 + 1 \mid n!.$$

13. A positive integer n will be called *strong* if it has the property that $p \mid n$ implies $p^2 \mid n$ for every prime p. Prove that there are infinitely many pairs of consecutive integers both being strong numbers.

14. Prove that for every $n > 0$, there is a prime number

$$p < 2006n^{\frac{3}{4}}$$

such that $-n$ is a nonquadratic residue mod p.

15. The numbers $a_1, a_2, \ldots, a_{2002}$ are such that the number

$$a_1^n + a_2^n + \ldots + a_{2002}^n$$

is a perfect square for every $n > 0$. What is the smallest number of null terms in the sequence?

16. Prove that all but finitely many positive integers can be expressed as the sum of different perfect squares.

17. Is it possible to find 100 positive integers not exceeding 25,000 such that all pairwise sums are different?

18. Find all squares that are written in base ten with a few sixes and one four.

19. For which positive integers n can the set $\{1, 2, \ldots, 2n\}$ be partitioned into n two element subsets so that the sum of the two members in each set is a perfect square?

20. Let $n \geq 1$ be a natural number. Prove that the set $\{1^2, 2^2, \ldots, n^2\}$ of the first n perfect squares can be partitioned into four subsets each having the same sum of elements if and only if n is either of the form $n = 8k - 1$, or of the form $n = 8k$, $k \geq 2$ being a positive integer.

21. Is there a polynomial $P(X, Y, Z)$ in three variables with integer coefficients such that the set of the values $P(x, y, z)$, for positive integers x, y, and z is exactly the set of the non-square positive integers?

22. Find all arithmetic progressions $(a_n)_{n \geq 1}$ such that $a_1 + \cdots + a_n$ is a square for all n.

Solutions

1. For every n, we have

$$n(n+1)(n+2)(n+3)+1 = \left(n^2+3n\right)\left(n^2+3n+2\right)+1 = \left(n^2+3n+1\right)^2.$$

2. Never. Suppose, without loss of generality, that $m \geq n$. In this case,

$$m^2 < m^2+n \leq m^2+m < (m+1)^2,$$

hence m^2+n is not a perfect square.

3. (Bogdan Enescu) Suppose that this is not possible. If 6 occurs after 1, then we can pick the number 16. So 6 occurs before 1. If 4 occurs after 6, then we can pick 64, hence 4 is before 6. If 9 occurs after 4, we can take 49, hence 9 is before 4. Now we know the order 9-4-6-1. We can pick now 961, which is a contradiction.

4. Since the last two digits are 1,

$$111\ldots111 \equiv 11 \equiv 3 \pmod 4).$$

Such numbers cannot be expressed as the sum of two perfect squares since the only possible remainders when a perfect square is divided by 4 are 0 and 1.

5. Note that 256 and 625 is a good pair. By adding the same (even) number of 0s at the end of these numbers generates infinitely many such pairs.

6. The idea here is to use the sum of digits. But we must be careful, because the sum of digits of this number is not

$$1^2+2^2+\ldots+99^2$$

since most of these terms are not digits! However, our number is congruent mod 9 to this sum (which is congruent to 6 mod 9) because every number is congruent mod 9 with its sum of digits. Hence our number is a multiple of 3, but not a multiple of 9, so it is not a perfect square.

7. Let

$$n = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$$

It is well-known that the number of positive divisors of n is

$$d(n) = (a_1+1)(a_2+1)\ldots(a_k+1).$$

This number is odd iff all $a_i + 1$ are odd or all a_i are even, i.e., n is a perfect square. Another way to put it is to group all divisors of n in pairs like $\left\{d, \frac{n}{d}\right\}$. If n is a perfect square, then the middle pair is $(\sqrt{n}, \sqrt{n})$, so there is exactly one repetition, hence $d(n)$ is odd. If n is not a perfect square, there are no repetitions, hence $d(n)$ is even.

8. If n is perfect square, then it is obvious. If n is not a perfect square, then we have seen at the previous problem that $d(n)$ is even, hence $n^{d(n)}$ is a perfect square.

9. All positive integers except those of the form $4k+2$. Because 0 and 1 are the only possible remainders when a perfect square is divided by 4, it is easy to see that the difference of two perfect squares is not of the form $4k+2$. Conversely, every positive integer is either odd, or of the form $4k$. We have
$$(k+1)^2 - k^2 = 2k+1$$
and
$$(k+1)^2 - (k-1)^2 = 4k,$$
hence our solution is complete.

10. The problem follows immediately from the previous one. Another solution is to use a simple identity:
$$\left(a^2 - b^2\right)\left(c^2 - d^2\right) = (ac+bd)^2 - (ad+bc)^2.$$

11. This result is due to Erdős. Let us call any positive integer with the desired property *good*. We prove that if n is good, then $n+4$ is also good. Let
$$n = \pm 1^2 \pm 2^2 \pm \ldots \pm k^2$$
Because of the identity
$$(k+1)^2 - (k+2)^2 - (k+3)^2 + (k+4)^2 = 4,$$
we have
$$n+4 = \pm 1^2 \pm 2^2 \pm \ldots \pm k^2 + (k+1)^2 - (k+2)^2 - (k+3)^2 + (k+4)^2,$$
hence $n+4$ is good. Now we only have to prove that 0, 1, 2, 3, 4, are good, which is easily checked. We leave this as an exercise for our readers.

12. As we have stated in this chapter, the negative Pell equation

$$x^2 - 5y^2 = -1$$

has infinitely many solutions. For large enough x and y, $x > 2y$ and

$$x^2 + 1 = 5y^2 \mid (2y)! \mid x!,$$

so we are done.

13. We present a solution using Pell's equation, though it is not the only possible solution. All we have to do is think about the Pell equation

$$x^2 - 8y^2 = 1,$$

which solves the problem since x^2 and $8y^2$ are always strong.

14. (Adrian Zahariuc) Take the largest nonnegative integer a such that

$$N = 4n - \left(4a^2 + 1\right)^2 \geq 0.$$

By straightforward calculations, $N < 2006n^{3/4}$.
Since $N > 0$ and $N \equiv 3 \pmod 4$, there is a prime divisor $p \equiv 3 \pmod 4$ of N. We claim p has the desired property. Of course,

$$p \leq N < 2006n^{3/4}.$$

Suppose, by way of contradiction, that there is a $k \in \mathbb{Z}$ such that

$$p \mid k^2 + n \Rightarrow p \mid 4k^2 + 4n = 4k^2 + \left(4a^2 + 1\right)^2 + N \Rightarrow p \mid 4k^2 + \left(4a^2 + 1\right)^2,$$

and since $p \equiv 3 \pmod 4$, $p \mid 2k$ and $p \mid 4a^2 + 1$ which is impossible since $p \equiv 3 \pmod 4$.

15. (Gabriel Dospinescu) The answer is 66. This can obviously be achieved by 66 0s and 1936 1s. Now let $a_1 \leq a_2 \leq \ldots \leq a_k$ be the nonzero members of the sequence. Hence $a_1^n + \ldots + a_k^n$ is always perfect square. We claim that k is a perfect square, which is enough to solve the problem. For every prime number $p > a_k$, we have $(p, a_i) = 1$ for all a_i, hence

$$a_1^{p-1} + \ldots + a_k^{p-1} \equiv k \pmod p$$

which means that k is a quadratic residue modulo p for every large enough prime p. Let

$$k = 2^u m^2 q_1 q_2 \ldots q_t, u \in \{0, 1\}$$

and $q_1, q_2, \ldots, q_t$ odd primes. Suppose that $t \geq 1$. For $p > a_k$, we have

$$\left(\frac{k}{p}\right) = \left(\frac{2}{p}\right)^u \left(\frac{q_1}{p}\right) \cdots \left(\frac{q_t}{p}\right)$$

$$= (-1)^{u\frac{p^2-1}{8}} (-1)^{\frac{(p-1)(q_1-1)}{4} \cdots \frac{(p-1)(q_t-1)}{4}} \left(\frac{p}{q_1}\right) \cdots \left(\frac{p}{q_t}\right).$$

Taking $p \equiv 1 \pmod 8$, we assure that

$$\left(\frac{k}{p}\right) = \left(\frac{p}{q_1}\right) \cdots \left(\frac{p}{q_t}\right).$$

If r is a quadratic nonresidue modulo q_1, if we take p such that

$$p \equiv r \pmod{q_1} \text{ and } p \equiv 1 \pmod{q_i}$$

for $i \geq 2$, then it is clear that $\left(\frac{k}{p}\right) = -1$, which leads to a contradiction. The existence of such p is guaranteed by the Chinese Remainder Theorem and Dirichlet's Theorem. Hence $t = 0$. It is easy to see that $u = 0$ as well. Hence $k = m^2$ and the proof is complete.

16. **Solution I.** (Radu Todor, IMO 2000 Shortlist) Take a positive integer N such that

$$N = a^2 + b^2 \quad \text{and} \quad 2N = c^2 + d^2$$

and a, b, c, d are relatively prime (for example, we could take $N = 29$). For any positive integer m, consider its representation as sum of different powers of 2:

$$m = \sum 2^{x_i}.$$

Grouping the even and the odd powers we get

$$m = \sum 4^{y_i} + 2 \sum 4^{z_i}.$$

Now, we have

$$4Nm = \sum \left(2^{y_i+1}a\right)^2 + \sum \left(2^{y_i+1}b\right)^2 + \sum \left(2^{z_i+1}c\right)^2 + \sum \left(2^{z_i+1}d\right)^2,$$

so we managed to express $4Nm$ as the sum of some different even perfect squares.

Take an arbitrary positive integer

$$n > K := 1^2 + (2N+1)^2 + (2 \cdot 2N+1)^2 + \ldots + (2N(4N-2)+1)^2.$$

Let $n = 4Nq + r$, $0 \leq r < 4N$. Because

$$r \equiv 1^2+(2N+1)^2+(2\cdot 2N+1)^2+\ldots+(2N(r-1)+1)^2 := M \pmod{4N},$$

we can write $n = 4Nk + M$, but $4Nk$ is the sum of some different even perfect squares and M is the sum of some different odd perfect squares, so we are done because all $n > K$ have the desired property.

Solution II. We use the following:

Lemma. Suppose $(a_n)_{n\geq 1}$ is a sequence of positive integers with the properties:

i) There exist positive integers p, q, and s such that $p \leq q$ and each integer in the interval $[p, q]$ is a sum of distinct terms of the sequence $(a_n)_{n\geq 1}$ among $a_1, \ldots, a_s$.

ii) For the above presumed p, q, and s, we have

$$a_{s+t} \leq a_{s+1} + \cdots + a_{s+t-1} + q - p$$

for each integer $t \geq 1$ (for $t = 1$, this means $a_{s+1} \leq q - p$, that is, the sum from the right is considered empty).

Then each integer at least equal to p is the sum of a few distinct terms of the sequence $(a_n)_{n\geq 1}$.

Proof. We show that each integer from the interval $[p, q + a_{s+1} + \cdots + a_{s+t}]$ is a sum of distinct terms of the sequence $(a_n)_{n\geq 1}$ with indices at most equal to $s + t$; we prove this assertion by inducting on t.

For $t = 0$ hypothesis i) says that this is true. Assume the claim is true for $t-1$ and prove it for $t \geq 1$. If x is an integer from the interval $[p, q+a_{s+1}+\cdots+a_{s+t}]$, two possibilities occur: x can be from $[p, q+a_{s+1}+\cdots+a_{s+t-1}]$, and in this case, the induction hypothesis solves the problem; or, x can be in the interval $[q + a_{s+1} + \cdots + a_{s+t-1}, q + a_{s+1} + \cdots + a_{s+t}]$, in which case, $x - a_{s+t}$ belongs to $[q + a_{s+1} + \cdots + a_{s+t-1} - a_{s+t}, q + a_{s+1} + \cdots + a_{s+t-1}]$. But, because of the hypothesis ii), this interval is included in $[p, q + a_{s+1} + \cdots + a_{s+t-1}]$, hence, by the induction hypothesis, $x - a_{s+t}$ is a sum of some terms of $(a_n)_{n\geq 1}$ with indices at most equal to $s+t-1$, which ends the proof.

One can note that the following variant of the above lemma holds: if $(a_n)_{n\geq 1}$ is a sequence of positive integers having the property i) from the lemma, and property ii′) $a_{s+1} \leq q - p$ and $a_{n+1} \leq 2a_n$ for all $n \geq s + 1$, then each positive integer at least equal to p is the sum of some distinct terms of the sequence $(a_n)_{n\geq 1}$. Indeed, the new hypothesis ii′) allows us to show that ii) holds too, by an easy induction on t (the reader will surely be able to do that). In this form it was proved by Richert in 1949. We use these results to show that every positive integer at least equal to 129 is the sum of some *distinct* squares. In order to do that, we first let the reader verify that every positive integer from the interval $[129, 298]$ can be represented as the sum of a few distinct squares among $1^2, \dots, 12^2$. For example, $129 = 10^2+5^2+2^2$, and $298 = 12^2+10^2+7^2+2^2+1^2$. Thus we apply the lemma for the sequence $(a_n)_{n\geq 1}$ of the squares ($a_n = n^2$, for all $n \geq 1$), with $p = 129$, $q = 298$, and $s = 12$. We prefer to use the theorem of Richert instead of the lemma, namely we still have to observe that $a_{s+1} = a_{13} = 169 = 298 - 129 = q - p$, and that the inequality $a_{n+1} \leq 2a_n \Leftrightarrow (n+1)^2 \leq 2n^2$ holds for all $n \geq 3$ (we only need it for $n \geq 12$). According to our lemma, any integer greater than or equal to 129 is the sum of a few distinct squares, which we intended to prove. Actually, Sprague proved in 1948 that the only positive integers which are *not* sums of distinct squares, are 2, 3, 6, 7, 8, 11, 12, 15, 18, 19, 22, 23, 24, 27, 28, 31, 32, 33, 43, 44, 47, 48, 60, 67, 72, 76, 92, 96, 108, 112, and 128 (sequence A001422 in Sloane's On-Line Encyclopedia of Integer Sequences).

By the way, the lemma can be improved to the following result:

Lemma. Suppose $(a_n)_{n\geq 1}$ is a sequence of positive integers with the properties:

i) There exist positive integers p, q, and s such that $p \leq q$ and each integer in the interval $[p, q]$ is a sum of distinct terms of the sequence $(a_n)_{n\geq 1}$ among $a_1, \dots, a_s$.

ii) For these p, q, and s we have

$$a_{s+t} \leq a_{s+1} + \cdots + a_{s+t-1} + q - p$$

for each integer $t \geq 1$.

iii) $(a_1 + \cdots + a_s)/2 \leq q$.

iv) The sequence $(a_n)_{n\geq 1}$ has infinitely many odd terms.

Then for any integer k, there are infinitely many m such that

$$k = \pm a_1 \pm a_2 \pm \cdots \pm a_m$$

for a suitable choice of the plus/minus signs.

Proof. As we have already seen, any integer $\geq p$ is a sum of a few distinct terms of the sequence $(a_n)_{n\geq 1}$. Also note that hypothesis iii) immediately implies that

$$\frac{a_1 + \cdots + a_m}{2} \leq q + a_{s+1} + \cdots + a_m$$

for all $m \geq s$.

Clearly, it suffices to prove the lemma for nonnegative integers k (for negative k, we only change the signs in the representation of $-k$). For infinitely many (large enough) m, $a_1 + \cdots + a_m$ has the same parity as k (this is due to hypothesis iv)) and is sufficiently large for

$$\frac{a_1 + \cdots + a_m - k}{2} \geq p$$

to hold. Therefore $(a_1 + \cdots + a_m - k)/2$ is a positive integer at least equal to p, and less than

$$\frac{a_1 + \cdots + a_m}{2} \leq q + a_{s+1} + \cdots + a_m;$$

according to what we just proved, this number is the sum of some terms of the sequence $(a_n)_{n\geq 1}$, with indices not exceeding m:

$$\frac{a_1 + \cdots + a_m - k}{2} = a_{i_1} + \cdots + a_{i_j},$$

with $1 \leq i_1 < \cdots < i_j \leq m$. This offers the representation

$$k = a_1 + \cdots + a_m - 2(a_{i_1} + \cdots + a_{i_j}),$$

as intended, and finishes the proof of the lemma.

In order to apply this improved lemma to the sequence of squares (and to conclude that any integer k has infinitely many representations of the form $k = \pm 1^2 \pm \cdots \pm m^2$) we must change the value of q to 325, for the inequality iii) to be true (as an equality). Fortunately, this does not affect the truth of i) and ii), with the same $s = 12$, as the reader can check (perhaps with the help of a computer). However, this is not the most clever proof of this result for the sequence of squares (see problem 11). Instead, the reader might like to try to use the lemma for the sequence of *perfect powers* (with exponent at least 2), starting $a_1 = 1$, $a_2 = 4$, $a_3 = 8$, $a_4 = 9$, $a_5 = 16$, $a_6 = 25$, $a_7 = 27$, $a_8 = 32$, $a_9 = 36$, $a_{10} = 49$, and so on. He/she could show that this sequence satisfies the hypotheses of the improved lemma with $p = 24$, $q = 56$, $s = 7$. Thus, every integer k has infinitely many expressions of the form $k = \pm 1 \pm 4 \pm 8 \pm 9 \pm \cdots$. As a final hint, note that $a_{n+1} \leq 2a_n$ holds for this sequence, too, starting with $n = 2$.

17. (IMO 2001 Shortlist) Yes, it is possible. We show that for every prime p, there are p such numbers not exceeding $2p^2$. This is enough since

$2 \cdot 101^2 < 25{,}000$. Let $\overline{k}$ denote the remainder when k is divided by p. We claim that the numbers

$$2kp + \overline{k^2}, \quad k = 1, 2, \ldots, p,$$

have the desired property. Suppose that

$$2ap + \overline{a^2} + 2bp + \overline{b^2} = 2cp + \overline{c^2} + 2dp + \overline{d^2},$$

with $a, b, c, d \in \{1, 2, \ldots, p\}$. Then

$$2p(a+b) + \left(\overline{a^2} + \overline{b^2}\right) = 2p(c+d) + \left(\overline{c^2} + \overline{d^2}\right),$$

hence $a + b = c + d$ and

$$\overline{a^2} + \overline{b^2} = \overline{c^2} + \overline{d^2} \Rightarrow a^2 + b^2 \equiv c^2 + d^2 \pmod{p}.$$

From these, it is easy to conclude that $\{a, b\} = \{c, d\}$, hence our solution is complete.

18. Such a square cannot have the last two digits 66 or 46, because in that case it would be divisible by 2, but not by 4 (impossible for a square). Thus it must be a number of the form $N = 6\ldots64$. Because the number formed by the last four digits is $6664 = 8 \cdot 833$ is divisible by 8, but not by 16, so is N *if* it has at least four digits (therefore it is not a square). We remain with 664 and 64, of which, of course, only 64 is a perfect square — and this is the answer to our problem.

19. (Problem 1768, proposed by G. R. A. 20 Problem Solving Group, *Mathematics Magazine* 2/2007, solved by John Christopher in the same magazine, 2/2008) The answer is: for all $n \in \{4, 7, 8, 9\} \cup \{12, 13, \ldots\}$ and the idea is to use induction. Suppose, for the moment, that we found partitions as required for all $12 \le n \le 29$. Let $m \ge 30$ be given and assume that for all $12 \le l \le m - 1$, the set $\{1, 2, \ldots, 2l\}$ admits such a partition; we prove that $\{1, 2, \ldots, 2m\}$ has such a partition, too.

    Consider the unique positive integer k such that

$$\frac{(2k+1)^2}{2} < 2m < \frac{(2k+3)^2}{2}$$

(thus, we frame $4m$ between two consecutive odd squares).
From $m \ge 30$, $k \ge 4$ follows, and this implies $k \ge 1/2 + 2\sqrt{2}$, thus $2k^2 - 2k - 7/2 \ge 12$, yielding

$$(2k+1)^2 - 2m > (2k+1)^2 - \frac{(2k+3)^2}{2} = 2k^2 - 2k - \frac{7}{2} \ge 12,$$

thus $(2k+1)^2 - 2m - 1 \geq 12$. On the other hand, the first inequality from above implies $(2k+1)^2 - 2m - 1 < (2k+1)^2 - 2m < 2m$. Of course, $(2k+1)^2 - 2m - 1$ is an even number, hence, according to the induction hypothesis, the set $\{1, 2, \ldots, (2k+1)^2 - 2m - 1\}$ can be partitioned into two element subsets with the sum of elements in each subset a perfect square. Also, the set $\{(2k+1)^2 - 2m, (2k+1)^2 - 2m + 1, \ldots, 2m\}$ can be partitioned like this by putting together in each set the elements that sum to $(2k+1)^2$ (the first and the last, the second and the second to last, and so on). This shows that the set $\{1, 2, \ldots, 2m\}$ has such a partition, too, and finishes the proof of the inductive step. In order to completely solve the problem one has to see that partitions as the problem statement requires are not possible for $n \in \{1, 2, 3, 5, 6, 10, 11\}$ and to provide such partitions for $n \in \{4, 7, 8, 9\} \cup \{12, 13, \ldots, 29\}$.

We prove the impossibility of finding a partition only for $n = 11$; for smaller values we proceed analogously, and, in principle, the proofs are simpler. So, suppose there exists a partition of $\{1, 2, \ldots, 22\}$ into two element subsets with sum of elements in every subset a perfect square. Then 18 must be in the same class of the partition with 7 (because if 18 sums with another number from $\{1, 2, \ldots, 22\}$ to a perfect square, that square must be 25; for 36, 18 would be needed as the other summand, and 49 is already too large). Similarly, because 7 is already taken, it cannot be together with 9, therefore 9 must be in the same class as 16. Then 20 must be together with 5 (it cannot be with 16 anymore). Now 11 could be in the same class with either 5 or 14, but 5 is already taken; so, 11 is with 14, and 2 remains without a partner.

We will not show all partitions for $n \leq 30$ that the reader is invited to find by himself or herself (because they exist!); we only provide one example, namely:

$$\begin{aligned}\{1, 2, \ldots, 26\} &= \{1, 24\} \cup \{2, 14\} \cup \{3, 22\} \cup \{4, 21\} \cup \{5, 20\} \\ &\cup \{6, 19\} \cup \{7, 18\} \cup \{8, 17\} \cup \{9, 16\} \cup \{10, 15\} \\ &\cup \{11, 25\} \cup \{12, 13\} \cup \{23, 26\}.\end{aligned}$$

20. Let us denote by $P(n)$ the statement: the set $\{1^2, 2^2, \ldots, n^2\}$ of the first n perfect squares can be partitioned into four subsets, each of which has the same sum of elements; first, we prove that, if $P(n)$ holds, then necessarily n is of the form $8k - 1$ or $8k$, with $k \geq 2$ a natural number.

    Indeed, suppose $P(n)$ is true; then, evidently, the sum of the first n squares must be divisible by 4, which means that $n(n+1)(2n+1)/24$ is a natural number.
    Consequently 8 is a divisor of the product $n(n+1)(2n+1)$; but the last

factor of this product is always odd, and $n, n+1$ are relatively prime numbers, so we have either $8 \mid n$, or $8 \mid (n+1)$, as stated. This means that n is either of the form $8k$ or of the form $8k-1$, but we still have to prove that k must be at least 2. Suppose $k=1$; this means the sets

$$\{1^2, 2^2, \ldots, 7^2\} \quad \text{and} \quad \{1^2, 2^2, \ldots, 8^2\}$$

could be partitioned as in the problem statement. Then, for the first set, the sum of the elements of any partition's subset should be 35, which is impossible (since one of the subsets contains the number 49); for the second one, the sum of the elements of any partition's subset should be 51, which is also impossible, because of the number $8^2 = 64$. Therefore, $k \geq 2$ follows in either case.

Now we demonstrate the sufficiency of the conditions $n = 8k$ or $n = 8k-1$, $k \in \mathbb{N}$, $k \geq 2$ with the following induction schema: first, observe that if $P(n)$ is true, then $P(n+32)$ also holds true. The partition

$$\begin{aligned}
&\{(n+1)^2, (n+2)^2, \ldots, (n+32)^2\} \\
&= \{(n+1)^2, (n+7)^2, (n+12)^2, (n+14)^2, \\
&\quad (n+20)^2, (n+22)^2, (n+25)^2, (n+31)^2\} \\
&\cup \{(n+2)^2, (n+8)^2, (n+11)^2, (n+13)^2, \\
&\quad (n+19)^2, (n+21)^2, (n+26)^2, (n+32)^2\} \\
&\cup \{(n+3)^2, (n+5)^2, (n+10)^2, (n+16)^2, \\
&\quad (n+18)^2, (n+24)^2, (n+27)^2, (n+29)^2\} \\
&\cup \{(n+4)^2, (n+6)^2, (n+9)^2, (n+15)^2, \\
&\quad (n+17)^2, (n+23)^2, (n+28)^2, (n+30)^2\}
\end{aligned}$$

shows how a set of 32 consecutive squares can be partitioned in four classes, each one having the same sum of elements. Thus, if we have the required partition for the set $\{1^2, 2^2, \ldots, n^2\}$, it is easy to obtain a partition for $\{1^2, 2^2, \ldots, n^2, (n+1)^2, \ldots, (n+32)^2\}$ with the same property.

Now, in order to finish the proof, it would be enough to prove that $P(15)$, $P(16)$, $P(23)$, $P(24)$, $P(31)$, $P(32)$, $P(39)$, $P(40)$ are true; and they are true, because of the partitions

$$\begin{aligned}
\{1^2, 2^2, \ldots, 15^2\} &= \{1^2, 7^2, 8^2, 14^2\} \cup \{2^2, 9^2, 15^2\} \\
&\qquad \cup \{3^2, 6^2, 11^2, 12^2\} \cup \{4^2, 5^2, 10^2, 13^2\}; \\
\{1^2, 2^2, \ldots, 16^2\} &= \{1^2, 6^2, 9^2, 16^2\} \cup \{2^2, 4^2, 8^2, 11^2, 13^2\} \\
&\qquad \cup \{3^2, 5^2, 12^2, 14^2\} \cup \{7^2, 10^2, 15^2\};
\end{aligned}$$

$$\begin{aligned}\{1^2,2^2,\ldots,23^2\} &= \{1^2,3^2,10^2,13^2,19^2,21^2\} \cup \{2^2,8^2,22^2,23^2\}\\ &\cup \{4^2,5^2,9^2,11^2,15^2,17^2,18^2\}\\ &\cup \{6^2,7^2,12^2,14^2,16^2,20^2\};\\ \{1^2,2^2,\ldots,24^2\} &= \{1^2,5^2,7^2,10^2,13^2,15^2,16^2,20^2\} \cup \{4^2,14^2,22^2,23^2\}\\ &\cup \{2^2,3^2,11^2,17^2,19^2,21^2\} \cup \{6^2,8^2,9^2,12^2,18^2,24^2\};\\ \{1^2,2^2,\ldots,31^2\} &= \{1^2,2^2,3^2,4^2,14^2,24^2,29^2,31^2\}\\ &\cup \{5^2,6^2,10^2,15^2,16^2,19^2,21^2,22^2,26^2\}\\ &\cup \{7^2,12^2,13^2,17^2,18^2,27^2,30^2\}\\ &\cup \{8^2,9^2,11^2,20^2,23^2,25^2,28^2\};\end{aligned}$$

and, of course,

$$\begin{aligned}\{1^2,2^2,\ldots,32^2\} &= \{1^2,7^2,12^2,14^2,20^2,22^2,25^2,31^2\}\\ &\cup \{2^2,8^2,11^2,13^2,19^2,21^2,26^2,32^2\}\\ &\cup \{3^2,5^2,10^2,16^2,18^2,24^2,27^2,29^2\}\\ &\cup \{4^2,6^2,9^2,15^2,17^2,23^2,28^2,30^2\};\end{aligned}$$

finally, we have

$$\begin{aligned}\{1^2,2^2,\ldots,39^2\} &= \{1^2,8^2,11^2,15^2,16^2,19^2,27^2,28^2,35^2,37^2\}\\ &\cup \{2^2,5^2,20^2,29^2,30^2,38^2,39^2\}\\ &\cup \{3^2,6^2,7^2,12^2,13^2,14^2,17^2,21^2,22^2,23^2,26^2,32^2,33^2\}\\ &\cup \{4^2,9^2,10^2,18^2,24^2,25^2,31^2,34^2,36^2\}\end{aligned}$$

and

$$\begin{aligned}\{1^2,2^2,\ldots,40^2\} &= \{1^2,6^2,18^2,20^2,32^2,34^2,35^2,37^2\}\\ &\cup \{2^2,7^2,14^2,15^2,16^2,28^2,30^2,39^2,40^2\}\\ &\cup \{3^2,4^2,5^2,9^2,13^2,21^2,22^2,27^2,29^2,36^2,38^2\}\\ &\cup \{8^2,10^2,11^2,12^2,17^2,19^2,23^2,24^2,25^2,26^2,31^2,33^2\},\end{aligned}$$

finishing the proof.

21. **Solution I.** (mathmanman, AoPS forum) Yes, there is. In this first solution we use the fact that the positive integer n is not a perfect square if and only if the Pell equation $u^2 - nv^2 = 1$ has a nontrivial solution (with u and v positive integers). We consider the three variable polynomial

$$P = Z^2(X^2 - ZY^2 - 1)^2 + Z.$$

If n is not a perfect square, let (u, v) be a solution in positive integers of the equation $u^2 - nv^2 = 1$, and we clearly have $P(u, v, n) = n$, thus any non-square is a value of the polynomial. On the other hand, if m is a square, and $P(x, y, z) = m$, we surely have $|x^2 - zy^2 - 1| \geq 1$ (otherwise we would get $x^2 - zy^2 - 1 = 0$ and $m = P(x, y, z) = z$, hence the Pell equation $x^2 - my^2 = 1$ would have a nontrivial solution and m could not be a square). But in that case

$$(z|x^2 - zy^2 - 1|)^2 < P(x, y, z) < (z|x^2 - zy^2 - 1| + 1)^2,$$

which contradicts the fact that $P(x, y, z) = m$ is a square.

Solution II. (v_Enhance, AoPS forum) The second solution uses the fact that the positive integer n is not a perfect square if and only if it is of the form $a^2 + b$ for positive integers a and b with $1 \leq b \leq 2a$. Now let

$$Q = (1 - 2015(Z - 1)(Z - 2))((X + Y - 1)^2 + 2Y + Z - 2)$$

and note that for positive integers x, y and $z > 2$, $Q(x, y, z)$ is negative. We have

$$Q(x, y, 1) = (x + y - 1)^2 + 2y - 1 \text{ and } Q(x, y, 2) = (x + y - 1)^2 + 2y$$

and both these values are (strictly) between $(x + y - 1)^2$ and $(x + y)^2$, for positive integers x and y. That is, no value of Q can be a square. On the other hand, we have

$$Q\left(\frac{2a - b + 1}{2}, \frac{b + 1}{2}, 1\right) = a^2 + b$$

for odd b, and

$$Q\left(\frac{2a - b + 2}{2}, \frac{b}{2}, 2\right) = a^2 + b$$

for even b, showing that every value that is not a square is attained by Q.

22. We know that for any positive integer n, there exists a positive integer b_n such that $a_1 + \cdots + a_n = b_n^2$. Also, because $(a_n)_{n \geq 1}$ is an arithmetic progression, there are A and B (namely $A = d/2$ and $B = a_1 - d/2$, where d is the common difference of the progression) such that

$$a_1 + \cdots + a_n = An^2 + Bn$$

for all $n \geq 1$. Thus we get $An^2 + Bn = b_n^2$ for all positive integers n, hence

$$\lim_{n \to \infty} (b_{n+1} - b_n) = \lim_{n \to \infty} \frac{2An + A + B}{\sqrt{A(n + 1)^2 + B(n + 1)} + \sqrt{An^2 + Bn}} = \sqrt{A}.$$

We found that the sequence with general term $b_{n+1} - b_n$ has a finite limit and we know that it only consists of integers. It follows that, necessarily, this sequence is eventually constant (all terms, except finitely many of them are equal to the limit, which has to be an integer, too), therefore there exists a positive integer N such that $b_{n+1} - b_n = \sqrt{A}$ for all $n \geq N$. We get $b_n = b_N + (n - N)\sqrt{A} = Cn + D$ (with $C = \sqrt{A}$ and $D = b_N - N\sqrt{A}$), yielding $An^2 + Bn = C^2n^2 + 2CDn + D^2$ for every $n \geq N$. Because we obtained two polynomials whose values are equal for infinitely many values of the indeterminate, their coefficients must be respectively equal, that is, we get $A = C^2$, $B = 2CD$, and $D^2 = 0$. Finally, $A = C^2$, with integer C, and $B = 0$, meaning that, for the original progression, $a_1 = C^2$ and $d = 2C^2$, with integer C.

Conversely, one sees that with these initial conditions,

$$a_1 + \cdots + a_n = (nC)^2$$

is a perfect square for every positive integer n. Basically, only the progression consisting of all odd positive integers has the required property.

Chapter 4

Digital Sums

For each positive integer $A = \overline{a_1a_2\ldots a_n}$, denote by

$$S(A) = a_1 + a_2 + \ldots + a_n$$

the digital sum of A. We will establish the following properties of the digital sum function. For all positive integers A, B, we have

$$S(A + B) \leq S(A) + S(B), \tag{1}$$

$$S(A \cdot B) \leq S(A \cdot B). \tag{2}$$

By filling in with zeros, we can assume, without loss of generality, that A and B have the same number of digits. Let us denote

$$A = \overline{a_1a_2\ldots a_n}, \quad B = \overline{b_1b_2\ldots b_n}.$$

We will use the adding algorithm,

$$\begin{array}{r} a_1a_2\ldots a_n \\ +\ b_1b_2\ldots b_n \\ \hline c_0c_1c_2\ldots c_n \end{array}$$

We have

$$S(A) + S(B) - S(A + B) = \sum_{k=1}^{n}(a_k + b_k - c_k) \tag{3}$$

If $a_n + b_n \leq 9$, then $a_n + b_n - c_n = 0$. If $a_n + b_n \geq 10$, then

$$a_n + b_n - c_n = 10.$$

Further, $a_{n-1} + b_{n-1} - c_{n-1}$ cannot be less than -1. In conclusion, the digital sum of $A + B$ diminishes with 9, whenever we have $a_k + b_k \geq 10$.

By induction,

$$S(A_1 + A_2 + \ldots + A_n) \leq S(A_1) + S(A_2) + \ldots + S(A_n)$$

and for every positive integer n, $S(nA) \leq nS(A)$.

Now, we are in position to prove the inequality (2). In this sense,

$$\begin{aligned} S(AB) &= S[(10^{n-1}a_1 + 10^{n-2}a_2 + \ldots + 10a_{n-1} + a_n)B] \\ &= S(10^{n-1}a_1B + 10^{n-2}a_2B + \ldots + 10a_{n-1}B + a_nB) \\ &\leq S(10^{n-1}a_1B) + S(10^{n-2}a_2B) + \ldots + S(10a_{n-1}B) + S(a_nB) \\ &= S(a_1B) + S(a_2B) + \ldots + S(a_{n-1}B) + S(a_nB) \\ &\leq a_1S(B) + a_2S(B) + \ldots + a_{n-1}S(B) + a_nS(B) \\ &= (a_1 + a_2 + \ldots + a_n)S(B) = S(A)S(B). \end{aligned}$$

One of the most important arithmetical properties of the digital sum function S is the fact that $S(n) \equiv n \pmod 9$ for all n. Why is this so? Let

$$n = a_0 + 10a_1 + 10^2a_2 + \ldots + 10^ka_k.$$

In this case,

$$\begin{aligned} n - S(n) &= \left(a_0 + 10a_1 + 10^2a_2 + \ldots + 10^ka_k\right) - (a_0 + a_1 + \ldots + a_k) \\ &= 9a_1 + 99a_2 + \ldots + \left(10^k - 1\right)a_k, \end{aligned}$$

which is a multiple of 9, therefore our property is true.

Another curiosity about the digital sum, which is frequently used in mathematical competitions, is the following:

Proposition. *If* $N \leq 10^k - 1$, *then*

$$S\left(\left(10^k - 1\right)N\right) = 9k.$$

Suppose, without loss of generality, that 10 does not divide N. Let

$$N = \overline{b_1b_2\ldots b_k},$$

where some of the leading digits might be zero. It is more convenient and easier to compute a difference rather than a product:

$$S\left(\left(10^k - 1\right)N\right) = S\left(10^kN - N\right) = S(\overline{b_1b_2\ldots b_k\underbrace{00\ldots00}_{k \text{ digits}}} - \overline{b_1b_2\ldots b_k})$$

$$= S\left(\overline{b_1b_2\ldots b_{k-1}(b_k - 1)(9 - b_1)(9 - b_2)\ldots(9 - b_{k-1})(10 - b_k)}\right) = 9k,$$

so the proof of the proposition is complete.

Example 1. Evaluate $S(1)-S(2)+S(3)-S(4)+\ldots+S(2013)-S(2014)$.

Solution. This is more like a joke. Just note that $S(2N+1)=S(2N)+1$ for every natural number N (since the last digit of $2N$ is at most 8, hence there are no carries when we add $2N$ with 1); thus, of course, the sum is $S(1)+1006-S(2014)=1000$.

Example 2. Find a natural number N such that $s(N)=1996s(3N)$.

Solution. We are not asked to find *all* such numbers, therefore we will just guess that, for numbers of the form $N=3\ldots36$, $S(N)$ is big, while $S(3N)$ is small. (Note that $3N=10\ldots08$, with the same number of 0s as the number of 3s in N.) If k is the numbers of 3s, the equation reads $3k+6=1996\cdot 9$, whence $k=5986$.

Example 3. (Russian Olympiad) Let N be a positive integer with

$$S(N)=100 \text{ and } S(44N)=800.$$

Find $S(3N)$.

Solution. Let us examine the proof of $S(AB)\le S(A)S(B)$ in the particular case of $S(44N)$, taking into account the given facts about it and $S(N)$. Namely, we have:

$$\begin{aligned}800=S(44N)&=S(40N+4N)\le S(40N)+S(4N)=S(4N)+S(4N)\\&\le 2S(4N)\le 2\cdot 4S(N)=8S(N)=800.\end{aligned}$$

Of course, this means that all inequalities must, in fact, be equalities. In particular, we have $S(4N)=4S(N)$, which can hold if and only if N has all digits at most equal to 2 in order that there is no carry when we multiply 4 to N. But in that case, for the same reason, $S(3N)=3S(N)$, thus $S(3N)=300$ is the required answer.

Example 4. (Russian Olympiad) Does there exist a positive integer N such that $S(N)=1000$ and $S(N^2)=1000000$?

Solution. Yes, there exists such an integer; in fact, for every positive integer s, one can find a number N having the properties $S(N)=s$ and $S(N^2)=s^2$. We want again to have equality in some inequality of the type $S(AB)\le S(A)S(B)$ (this time for $A=B=N$), hence we look for a number N with digits as small as possible, that is, a number formed with 0s and 1s only. A moment of thinking shows that we can take

$$N=\sum_{i=0}^{s-1}10^{2^i}$$

(which is, indeed, a number with 2^s digits, of which s are 1s). We clearly have

$S(N) = s$ and we can compute

$$N^2 = \sum_{i=0}^{s-1} 10^{2^{i+1}} + 2 \sum_{0\le k<l\le s-1} 10^{2^k+2^l}.$$

Due to the uniqueness of the representation in base 2, all the exponents of 10 that appear in the above formula are distinct, therefore

$$S(N^2) = s \cdot 1 + \frac{s(s-1)}{2} \cdot 2 = s^2,$$

exactly what we intended to show.

Example 5. Find all positive integers N such that

$$N + S(N) - S(S(N)) = 2014.$$

Solution. Time to use $N \equiv S(N) \pmod 9$! So, if N is a solution, and r is the remainder of N (and $S(N)$) divided by 9, we must have $r + r - r \equiv 2014 \pmod 9$, hence $r = 7$. Also we clearly have $S(x) \le x$ for every natural number x, therefore $S(S(N)) - S(N) \le 0$ and $N \le 2014$. Because N has at most four digits, and $S(N) \equiv 7 \pmod 9$, $S(N)$ can only be one of the numbers $7, 16, 25, 34$. We obtain the solutions 2014 and 1996 ($S(N) = 16$ and $S(N) = 34$ don't yield solutions of the original equation.)

Example 6. Let $N = \overline{c_{n-1}\ldots c_1c_0}$ be the decimal representation of the natural number N. Prove that

$$S(kN) = \sum_{i=0}^{n-1} S(kc_i)$$

for either $k = 2$ or $k = 5$.

Solution. We have

$$N = \sum_{i=0}^{n-1} 10^i c_i.$$

We consider $kc_i = 10a_i + b_i$, where a_i and b_i are base-10 digits, for each $0 \le i \le n-1$, and we compute

$$kN = \sum_{i=0}^{n-1} 10^i(10a_i + b_i) = 10^n a_{n-1} + 10^{n-1}(a_{n-2} + b_{n-1}) + \ldots + 10(a_0 + b_1) + b_0.$$

Now, for $k = 2$, we have $a_i \in \{0, 1\}$ and $b_i \in \{0, 2, 4, 6, 8\}$ for all i, and for $k = 5$, we have $a_i \in \{0, 1, 2, 3, 4\}$ and $b_i \in \{0, 5\}$ for all i. In both cases we see that no $a_{i-1} + b_i$ can exceed 9, hence the sum of digits of $S(kN)$ is

$$S(kN) = a_{n-1} + (a_{n-2} + b_{n-1}) + \ldots + (a_0 + b_1) + b_0 = \sum_{i=0}^{n-1}(a_i + b_i) = \sum_{i=0}^{n-1} S(kc_i),$$

which is what we wanted to prove.

Example 7. Find the smallest positive integer N such that

$$S(N) - S(5N) = 2013.$$

Solution. Let $N = \overline{c_{n-1}\dots c_1c_0}$, and, as in the previous problem, let $5c_i = 10a_i + b_i$, with a_i and b_i being digits. Note that any a_i can be 0, 1, 2, 3, or 4, and any b_i is either 0 or 5. By the result that we just proved, the equation from the problem can be written as

$$\sum_{i=0}^{n-1} c_i - \sum_{i=1}^{n-1}(a_i + b_i) = 2013 \Leftrightarrow \sum_{i=0}^{n-1} a_i - 4\sum_{i=0}^{n-1}\frac{b_i}{5} = 2013.$$

In order to minimize N we have to minimize n (the number of digits), therefore we must have most of the a_is equal to 4. Also, we must have as many as possible of the b_is equal to 0, and the c_is as small as possible (therefore they must be 8s). Also, because $\sum_{i=0}^{n-1} a_i$ has to be 1 modulo 4, we see that a 2 must appear in N. The minimum is thus $N = 28\dots8$ with 503 digits of 8.

Example 8. Prove that if N has n digits and $S((10^{n-1}+1)N) = S(N)$, then $N = 10^n - 1$.

Solution. Let $N = \overline{c_{n-1}\dots c_0}$ as above; then

$$(10^{n-1}+1)N = \overline{c_{n-1}\dots c_0 0\dots 0} + \overline{c_{n-1}\dots c_0},$$

where the first summand ends in $n-1$ zeros. Clearly the given equality cannot hold if $c_0 + c_{n-1} \le 9$ (that is, if there isn't a carry when we add the digit c_0 of the first term with c_{n-1} from the second), and one can easily see that the equality doesn't hold when $c_1 \neq 9$ (that is, when the addition of the digits of immediately greater order doesn't provide a carry). So, we can assume that $c_0 + c_{n-1} \ge 9$ and, say $c_1 = \dots = c_k = 9$, for some $1 \le k \le n-1$.
If $k+1 \le n-1$,

$$(10^{n-1}+1)N = \overline{c_{n-1}\dots c_{k+2}(c_{k+1}+1)0\dots 0(c_0+c_{n-1}-10)c_{n-2}\dots c_0},$$

and the equality $S((10^{n-1}+1)N) = S(N)$ yields $c_{n-1} + \dots + c_k + c_0 = 9$, which is impossible as long as we know that $c_0 + c_{n-1} \ge 10$. Thus $k = n-1$ is necessary (i.e., all digits of N from c_1 to c_{n-1} are 9s), in which case,

$$(10^{n-1}+1)N = \overline{10\dots 0(c_0+c_{n-1}-10)c_{n-2}\dots c_0},$$

with $n-1$ 0s. Clearly now $S((10^{n-1}+1)N) = S(N)$ implies $c_0 = 9$, finishing the proof.

By the way, this result immediately solves the well-known problem that asks for those positive integers N with property that

$$S(N) = S(2N) = \ldots = S(N^2).$$

Using the fact that $S((10^n - 1)x)) = 9n$ for all $x \leq 10^n - 1$, we see that every number N of the form $N = 10^n - 1$ works. Conversely, if $S(kN) = S(N)$ for all $1 \leq k \leq N$, we can consider $k = 10^{n-1} + 1$ (with n the number of digits of N) and conclude that $N = 10^n - 1$. Note that we can choose this k because N has at n digits, and, obviously, it cannot be 10^{n-1}. Thus, the solutions to the problem are the numbers consisting of only nines (in their base-10 representation, of course).

Example 9. Show that we can find (for any given positive integer n) some natural numbers $a_1, \ldots, a_n$ such that $S(a_1) < S(a_2) < \ldots < S(a_n)$ and $S(a_i) = P(a_{i+1})$ for $i = 1, 2, \ldots, n$, where $a_{n+1} = a_1$ and $P(N)$ denotes the product of the digits of the natural number N.

Solution. We will search for numbers of the form $a_i = 2\ldots21\ldots1$ with k_i digits of 2 and l_i digits of 1, for all $1 \leq i \leq n$. We want the k_is and l_is to fulfill the conditions

$$2k_1 + l_1 < 2k_2 + l_2 < \ldots < 2k_n + l_n$$

and $2k_i + l_i = 2^{k_{i+1}}$ for $1 \leq i \leq n$. Thus, actually, the question is: can we find n positive integers $k_1, \ldots, k_n$ such that $k_2 < \ldots < k_n < k_1$ and $2^{k_{i+1}} \geq 2k_i \Leftrightarrow 2^{k_{i+1}-1} \geq k_i$ for all $1 \leq i \leq n$? (Of course, $k_{n+1} = k_1$, and the second series of inequalities ensures that, once the k_i chosen, we can define $l_i = 2^{k_{i+1}} - 2k_i$.)

The answer is yes, and we proceed as follows. Because $\lim\limits_{x\to\infty}(2^{x-1} - x) = \infty$, we can pick k_2 large enough such that the difference $2^{k_2-1} - k_2$ is sufficiently large in order that between k_2 and 2^{k_2-1}, there are at least $n-1$ distinct integers (for example, we ask this difference to be larger than $2n$, which is achievable). Next, we choose $n-1$ such integers, so we choose arbitrarily $k_3 < \ldots < k_n < k_1$ satisfying $k_2 < k_3 < \ldots < k_n < k_1 < 2^{k_2-1}$. So, the inequalities from the first set are fulfilled, and the first inequality from the second set is also verified. For $2 \leq i \leq n$, we have $2^{k_{i+1}-1} > 2^{k_i-1} \geq k_i$, according to the well-known inequality $2^{x-1} \geq x$ (for positive integers x), and this is what we wanted to prove.

For example, take $n = 3$ and $k_2 = 5$, in order to have $2^{k_2-1} - k_2 = 12$, a difference large enough to make us able to choose $k_3 = 7$ and $k_1 = 10$ (for example) such that we have $k_2 < k_3 < k_1 < 2^{k_2-1}$. Then define $l_1 = 2^{k_2} - 2k_1 = 12$, $l_2 = 2^{k_3} - 2k_2 = 118$, and $l_3 = 2^{k_1} - 2k_3 = 1010$. Then pick a_1 consisting of 10 digits of 2 and 12 digits of 1, a_2 formed with 5 digits of 2 and 118 digits of 1, and a_3 with 7 digits of 2 and 1010 digits of 1.

Example 10. (Yiu Tung Poon, Mathematics Magazine 4/2007, solved in 4/2008; but the problem also appears in the book from 2004 *Experimentation in Mathematics. Computational Paths to Discovery* by Jonathan Borwein, David Bailey, Roland Girgensohn; the problem with $g(n)$ — the number of digits of n that are greater than 4 — in place of $o(n)$ was proposed by Eugene Levine in the *College Mathematics Journal* from November 1988 and was also proposed by Doug Bowman and Tad White as problem 6609 in *The American Mathematical Monthly* from October, 1989) Let $o(N)$ be the number of odd digits of the positive integer N. Prove that

$$\sum_{n=1}^{\infty}\frac{o(2^n)}{2^n}=\frac{1}{9}.$$

Solution I. For positive integers n and j, let $f(n,j)$ be 1 if $[2^n/10^{j-1}]$ is odd, and let it be 0 otherwise; in other words, $f(n,j)$ is the remainder of $[2^n/10^{j-1}]$ when divided by 2 (by $[x]$, we denote the integral part of the real number x). Note that $f(n,j)$ is 1 precisely when the jth digit of 2^n, counted from the right, is odd. This is why

$$\sum_{n=1}^{\infty}\frac{o(2^n)}{2^n}=\sum_{n=1}^{\infty}\sum_{j=1}^{\infty}\frac{f(n,j)}{2^n}.$$

Interchanging the order of summation further yields

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{o(2^n)}{2^n}&=\sum_{n=1}^{\infty}\sum_{j=1}^{\infty}\frac{f(n,j)}{2^n}=\sum_{j=1}^{\infty}\sum_{n=1}^{\infty}\frac{f(n,j)}{2^n}\\&=\sum_{j=1}^{\infty}\left(\frac{1}{10^{j-1}}-\left[\frac{1}{10^{j-1}}\right]\right)\\&=\sum_{j=2}^{\infty}\frac{1}{10^{j-1}}=\frac{1}{9}.\end{aligned}$$

The equality used after interchanging the summation order is justified by the fact that $f(n,j)$ (actually being $[2^n/10^{j-1}]$ modulo 2) is given by

$$f(n,j)=\left[\frac{2^n}{10^{j-1}}\right]-2\left[\frac{[2^n/10^{j-1}]}{2}\right]=\left[\frac{2^n}{10^{j-1}}\right]-2\left[\frac{2^{n-1}}{10^{j-1}}\right]$$

(where, for the last equality, we used the general identity $[[x]/p]=[x/p]$ for real x and positive integer p). Thus, the partial sum of the inner series is telescoping like

$$\sum_{n=1}^{m}\frac{f(n,j)}{2^n}=\sum_{n=1}^{m}\left(\frac{1}{2^n}\left[\frac{2^n}{10^{j-1}}\right]-\frac{1}{2^{n-1}}\left[\frac{2^{n-1}}{10^{j-1}}\right]\right)=\frac{1}{2^m}\left[\frac{2^m}{10^{j-1}}\right]-\left[\frac{1}{10^{j-1}}\right],$$

therefore it sums to $1/10^{j-1} - [1/10^{j-1}]$ (which is, in fact, 0 for $j = 1$, and $1/10^{j-1}$ for $j \geq 2$). The proof is now complete.

Solution II. It is very easy to see that, for every positive integer N, $o(2N)$ equals the number of digits of N that are greater than 4 — this number will be further denoted by $g(N)$. (Each such digit of N produces, by multiplication with 2, an odd digit in $2N$.) Then it is again pretty easy to prove that $2S(N) - S(2N) = 9g(N)$ for all N. Indeed, every digit of N which is greater than 4 increases the expression $2S(N) - S(2N)$ by 9. To put it more formally, let

$$N = \overline{c_{k-1}\dots c_0},$$

and let $2c_i = 10a_i + b_i$, with $0 \leq a_i, b_i, c_i \leq 9$, for $0 \leq i \leq k-1$. We have

$$2N = 2\sum_{i=0}^{k-1} c_i 10^i = \sum_{i=0}^{k-1}(10a_i + b_i)10^i$$

$$= a_{k-1}10^k + (a_{k-2} + b_{k-1})10^{k-1} + \dots + (a_0 + b_1)10 + b_0,$$

and, because $a_{i-1} + b_i$ is never greater than 9 (a_i can only be 0 or 1, and b_i is always an even digit), we have

$$S(2N) = \sum_{i=0}^{k-1} a_i + \sum_{i=0}^{k-1} b_i = \sum_{i=0}^{k-1}(10a_i + b_i) - 9\sum_{i=0}^{k-1} a_i = 2S(N) - 9g(N).$$

The last equality follows from the simple observation that a_i is 0 or 1, according to whether $c_i \leq 4$, or $c_i > 4$.

Now we get the desired result by observing that the partial sums of the series to evaluate telescope:

$$\sum_{n=1}^{m} \frac{o(2^n)}{2^n} = \sum_{n=1}^{m} \frac{g(2^{n-1})}{2^n} = \frac{1}{9}\sum_{n=1}^{m}\left(\frac{S(2^{n-1})}{2^{n-1}} - \frac{S(2^n)}{2^n}\right) = \frac{1}{9}\left(1 - \frac{S(2^m)}{2^m}\right)$$

and by using the well-known fact that $\lim_{N\to\infty} S(N)/N = 0$ (Why?).

Note that this solution is the one that put the problem here. The sum of digits appears somehow unexpectedly. Maybe if the problem had been stated in the slightly more general form:

$$\sum_{n=1}^{\infty} \frac{o(2^n N)}{2^n} = \frac{1}{9}S(N)$$

it would have suggested the use of the sum of digits (and also the formula used for telescoping — if someone would have thought about this type of summation). The reader can now easily prove this generalization, or extend the problem to other bases.

Proposed Problems

1. If n and $3n$ have the same digital sum, prove that n is divisible by 9.

2. Let n be a three-digit number. Prove that $S(91n) \geq S(n)$. Find all three-digit numbers n such that $S(91n) = 5$.

3. Let N be a positive integer with the property that in its decimal representation, each digit is less than the next digit to its right. Find the digital sum of $9N$.

4. Find the digital sum of the number $9 \times 99 \times 9999 \times \ldots \times (10^{2^n} - 1)$.

5. Prove that there exist an infinite number of positive integers which are divisible by their digital sum and whose decimal representation does not contain zero.

6. Let n be a 1998-digit integer, divisible by 9. Denote by x its digital sum, by y the digital sum of x, and by z the digital sum of y. Find z.

7. A student writes all positive integers from 1 to 111 in some arbitrary order. Is it possible that the obtained number is a perfect square?

8. A student has 10 blue cards with the digits $0, 1, 2, \ldots, 9$ and 9 red cards with the sign '+' on each of them. Using all blue cards and some of the red cards, can he write an expression with the result 100?

9. Prove that there exist infinitely many numbers n for which
$$S(3^n) \geq S(3^{n+1}).$$

10. Let S be the set of those positive integers which consist only of 0s and exactly 1988 1s. Prove that there is some $n \in \mathbb{N}$ which does not divide any element of S.

11. Prove that for each positive integer n, we can find a multiple of 2^n having only the digits 1 and 2.

12. Prove that there exists a multiple of 5^{2000} whose decimal representation does not contain zero.

13. Let α and β be two integers obtained by permutations of the digits of the number 1234567. Prove that if α divides β, then $\alpha = \beta$.

14. Consider the number $N = 999\ldots99$ (999 digits). Find the value of n for which $9^n \mid N$ and $9^{n+1} \nmid N$.

15. a) The digits of a given integer are permuted to obtain a new number. Prove that the sum of the given number with the new number cannot be equal to $999\ldots99$ (1999 digits).

    b) The digits of a given integer are permuted to obtain a new number. Prove that if the sum of the given number with the new number is equal to 10^{2000}, then the given number is divisible by 10.

16. Are there 19 different positive integers with the same sum of digits, which add up to 1999?

17. Find all $n \geq 2$ such that $S(n) = S(2n) = S(3n) = \ldots = S(n^2)$.

18. Let n be a fixed positive integer. Denote by $f(n)$ the smallest k for which one can find a set $X \subset \mathbb{N}$ of cardinality n with the property that

$$S\left(\sum_{x\in Y} x\right) = k$$

    for all nonempty subsets Y of X. Prove that $C_1 \lg n < f(n) < C_2 \lg n$ for some constants C_1 and C_2.

19. Is there a power of 2 such that we can rearrange its digits in order to obtain another (different) power of 2?

20. (Laurenţiu Panaitopol, Romanian TST) Let a and b be real numbers with $a > 0$. Show that $[an + b]$ has the same sum of digits for infinitely many values of n, where $[x]$ is the integer part of the real number x.

21. (Laurenţiu Panaitopol, Romanian TST, 1983) Prove that the statement: "There exist natural n-digit numbers such that the sum of digits of such a number equals the product of those digits" is true for infinitely many n and is false for infinitely many n.

22. For a natural number N we denote by $a(N)$ and $b(N)$ the number of its decimal digits that are equal to $4, 5, 6$, and $7, 8, 9$ respectively. Also, let $c(N)$ be the number of digits of 3 and 6 that appear in maximal sequences of one of the forms $3\ldots3c$, with $c \in \{4,5,6,7,8,9\}$, or $3\ldots36\ldots6c$ with $c \in \{7,8,9\}$. Note that maximal means that to the left of the first 3 in the decimal representation of N there isn't another 3 and also note that the 6s are counted for both $a(N)$ and $c(N)$. Finally, let $d(N) = 9(a(N) + 2b(N) + c(N))$.

    Thus we have, for instance, $a(334591333668) = 4$, $b(334591333668) = 2$, and $c(334591333668) = 7$ (hence $d(334591333668) = 135$).

Evaluate

$$\sum_{n=1}^{\infty} \frac{d(3^n)}{3^n}.$$

23. (J. O. Shallit, *The American Mathematical Monthly*, Problem 6450, 1/1984, solved in 7/1985) a) Let $m \geq 2$ be a positive integer. Prove that

$$\sum_{n=1}^{\infty} \frac{n - m[n/m]}{n(n+1)} = \ln m.$$

b) Let $b \geq 2$ an integer, and let $S_b(n)$ be the sum of digits of n written in base b. Show that

$$\sum_{n=1}^{\infty} \frac{S_b(n)}{n(n+1)} = \frac{b}{b-1} \ln b.$$

(By $[x]$, we denote the integer part of x.)

Solutions

1. We have $n \equiv S(n) \equiv S(3n) \equiv 3n \pmod 9$, thus $9 \mid 2n$ and so $9 \mid n$.

2. We will use the known inequality:

$$S(mn) \leq S(m)S(n).$$

If $n = \overline{abc}$, then $1001n = \overline{abcabc}$, and further,

$$2S(n) = S(1001n) = S(11 \cdot 91n) \leq S(11)S(91n) = 2S(91n).$$

For the last part, $n \equiv 91n (\operatorname{mod} 9)$, so $S(n) \equiv S(91n)(\operatorname{mod} 9)$. But we have: $S(n) \leq S(91n) \leq 5$, thus $S(n) = 5$. Finally, $n = 122$ and $n = 221$.

3. Denote $N = \overline{a_1 a_2 \ldots a_n}$ with $a_1 < a_2 < \ldots < a_n$. Let us write the equality $9N = 10N - N$, as:

$$\begin{array}{rcccccc} & a_1 & a_2 & \ldots & a_n & 0 & - \\ & & a_1 & \ldots & a_{n-1} & a_n & = \\ 9N = & a_1 & (a_2 - a_1) & \ldots & (a_n - a_{n-1} - 1) & (10 - a_n) & \end{array}$$

and see that

$$S(9N) = a_1 + (a_2 - a_1) + \ldots + (a_{n-1} - a_{n-2}) + (a_n - a_{n-1} - 1) + (10 - a_n),$$

hence $S(9N) = 9$.

4. (USAMO 1992) Let us denote

$$\alpha_m = 9 \times 99 \times 9999 \times \ldots \times (10^{2^m} - 1),$$

for $m = 1, 2, \ldots, n$. By induction, α_m has $k = 2^{m+1} - 1$ digits. Then $\alpha_{n-1} \leq 10^{2^n} - 1$ and, due to the lemma from the beginning of this chapter, its digital sum will be $9 \cdot 2^n$.

5. We prove, by induction on n, that $3^{n+1} \mid 10^{3^{n-1}} - 1$.
Indeed, if $10^{3^{n-1}} - 1 = 3^{n+1} \cdot \alpha$, then

$$\begin{aligned}10^{3^n} - 1 &= (10^{3^{n-1}})^3 - 1 = (10^{3^{n-1}} - 1)(10^{2 \cdot 3^{n-1}} + 10^{3^{n-1}} + 1)\\ &= 3^{n+1}\alpha(10^{2 \cdot 3^{n-1}} + 10^{3^{n-1}} + 1).\end{aligned}$$

The number $10^{2 \cdot 3^{n-1}} + 10^{3^{n-1}} + 1$ is divisible by 3, because the sum of its digits is equal to 3. In conclusion, the numbers of the form $999\ldots99$ (3^{n-1} digits) are solutions of the problem.

6. First, z is a multiple of 9. We have $x \leq 1998 \cdot 9 = 17982$, therefore

$$y < 1 + 7 + 9 + 9 + 9 = 35 \Rightarrow z \leq 2 + 9 = 11,$$

so $z = 9$.

7. The answer is negative. Suppose, by way of contradiction, it is a perfect square x^2. The digital sum of this number is

$$S(x^2) = 1 + 2 + \ldots + (1 + 1 + 1) = S(1) + S(2) + \ldots + S(111),$$

but $S(n) \equiv n \pmod 9$, hence

$$x^2 \equiv 1 + 2 + \ldots + 111 = 111 \cdot 56 \pmod 9$$

which means that $3 \mid x^2 \Rightarrow 3 \mid x$, but $9 \nmid x^2$, a contradiction.

8. The answer is negative and the idea is very similar to the one in the previous problem. In the given expression, each digit from 0 to 9 occurs exactly once, hence the sum of these numbers, s, should be congruent mod 9 with the sum of the digital sums of these numbers, which is $0 + 1 + 2 + \ldots + 9 = 45$, a multiple of 9. Hence, $9 \mid s$, so it cannot be 100.

9. (Kvant) Let us suppose, by way of contradiction, that there exists n_0 such that

$$S(3^{n+1}) > S(3^n)\ , \ \ \forall n \geq n_0.$$

Then $S(3^{n+1}) \geq S(3^n) + 9$ and by induction,

$$S(3^{n_0+m}) \geq S(3^{n_0}) + 9m,$$

for all positive integers m. On the other hand,

$$S(3^{n_0+m}) \leq 9(\lg 3^{n_0+m} + 1),$$

so

$$S(3^{n_0}) + 9m \leq 9(\lg 3^{n_0+m} + 1),$$

for any $m \in \mathbb{N}$, which is a contradiction.

10. (Tournament of Towns) The problem actually comes from a more general result regarding the digital sum:

    Lemma 1. *Any multiple of* $\underbrace{11\ldots11}_{k}$ *has digital sum at least* k.

    We will use the extremal principle. Suppose, by way of contradiction, that the statement is false and take M to be the smallest multiple of a such that $S(M) < k$, where $a = \underbrace{11\ldots11}_{k}$. Note that $S(ia) = ik$ for $i = 1, 2, \ldots, 9$. So $M \geq 10a > 10^k$. Therefore, $M = \overline{a_1a_2\ldots a_p}$, with $p \geq k+1$ and $a_p \neq 0$. Take the number $N = M - 10^{p-k}a$. Obviously, N is a multiple of a. We will try to prove that $S(N) < k$. In this way, we would contradict the minimality of M and the proof would be complete. But this is not hard at all since if $a_{k+1} < 9$, we have $S(N) = S(M) < k$ and if $a_{k+1} = 9$, we have $S(N) < S(M) < k$.

    Therefore, we can choose $n = 10^{1989} - 1$.

11. We will find by induction such a multiple of 2^n having n digits. Let us assume that

    $$\overline{a_1a_2\ldots a_n} = 2^n \cdot \alpha,$$

    with $a_i \in \{1, 2\}$, $1 \leq i \leq n$. Define

    $$b = \overline{1a_1a_2\ldots a_n} \quad \text{and} \quad c = \overline{2a_1a_2\ldots a_n}.$$

    It follows that:

    $$b = 2^n(\alpha + 5^n) \quad \text{and} \quad c = 2^n(\alpha + 2\cdot 5^n),$$

    so $2^{n+1} \mid b$ if α is odd and $2^{n+1} \mid c$ if α is even. Now the conclusion follows by induction.

12. We will prove by induction that for any integer $n \geq 1$, there exists a n-digit multiple of 5^n whose decimal representation contains only digits the 1, 2, 3, 4, and 5. Let us suppose that

$$\overline{a_1a_2\ldots a_n} = 5^n \cdot \alpha,$$

with $a_i \in \{1,2,3,4,5\}$, $1 \leq i \leq n$. Define

$$x_k = \overline{ka_1a_2\ldots a_n},\ 1 \leq k \leq 5.$$

We have:

$$x_k = 5^n(k \cdot 2^n + \alpha),$$

so take k such that $5 \mid k \cdot 2^n + \alpha$. This is always possible, because dividing the numbers $2^n + \alpha$, $2 \cdot 2^n + \alpha$, $3 \cdot 2^n + \alpha$, $4 \cdot 2^n + \alpha$, $5 \cdot 2^n + \alpha$ by 5, the obtained remainders are different.

The problem which requires to prove that 5^n has a n-digit multiple consisting only of the digits 1, 2, 3, 4, and 5 was given in the Romanian National Olympiad in 2005 and it is also quite classical. Another (similar) way to solve it is to prove that all n-digit numbers with digits 1, 2, 3, 4 and 5 give different residues when divided by 5^n. However, concerning the initial problem, a more general statement can be proved, namely, that every positive integer which is not divisible by 10 has a multiple which consists only of nonzero digits, but what is most interesting is the fact that, in order to prove it, one needs to prove the result first for powers of 2 and powers of 5 (so the given problem) and then extend it to the general case.

13. We see that $\alpha \equiv 1 \pmod 9$, $\beta \equiv 1 \pmod 9$, because they have the digital sum equal to $1+2+3+4+5+6+7 = 28$. If $\alpha = 9k+1$ and $\beta = 9p+1$, then

$$\beta = m\alpha \Rightarrow 9p + 1 = m(9k+1),$$

so $9 \mid m - 1$. It follows $m = 1$, thus $\alpha = \beta$.

14. We have $N = (9+1)^{999} - 1 = \displaystyle\sum_{k=1}^{999} \binom{999}{k} 9^k$, thus $n = 2$.

15. a) If $\overline{a_1a_2\ldots a_{1999}}$ is the given number, then the obtained number is

$$999\ldots99 - \overline{a_1a_2\ldots a_{1999}} = \overline{(9-a_1)(9-a_2)\ldots(9-a_{1999})}.$$

In particular,

$$a_1 + a_2 + \ldots + a_{1999} = (9 - a_1) + (9 - a_2) + \ldots + (9 - a_{1999}),$$

hence

$$2(a_1 + a_2 + \ldots + a_{1999}) = 9 \cdot 1999,$$

which is impossible.

b) Let $\overline{b_1b_2 \ldots b_{2000}}$ be the given number. If $b_{2000} \neq 0$, then

$$10^{2000} - \overline{b_1b_2 \ldots b_{2000}} = \overline{(9 - b_1) \ldots (9 - b_{1999})(10 - b_{2000})}$$

is the obtained number. In particular,

$$b_1 + b_2 + \ldots + b_{2000} = (9 - b_1) + \ldots + (9 - b_{1999}) + (10 - b_{2000}),$$

hence

$$2(b_1 + b_2 + \ldots + b_{2000}) = 9 \cdot 1999 + 10,$$

which is a contradiction.

16. (Russia) The answer is negative. Suppose, by way of contradiction, that there are $n_1 < n_2 < \ldots < n_{19}$ such that

$$S(n_1) = S(n_2) = \ldots = S(n_{19}) = k;$$

and

$$n_1 + n_2 + \ldots + n_{19} = 1999.$$

We have

$$1999 = n_1 + n_2 + \ldots + n_{19} \equiv S(n_1) + S(n_2) + \ldots + S(n_{19}) = 19k \pmod 9,$$

so $k \equiv 1 \pmod 9$. On the other hand,

$$19n_1 < n_1 + n_2 + \ldots + n_{19} = 1999 \Rightarrow n_1 \leq 100,$$

so $s(n_1) \leq 18$, i.e., $k \leq 18$. Hence, $k \in \{1, 10\}$. If $k = 1$, then all n_i are powers of 10, but there are only 4 different powers of 10 not exceeding 1999, which is a contradiction. Hence $k = 10$. The first 20 numbers with the digital sum equal to 10 are

$$19, 28, \ldots, 91, 109, 118, 127, \ldots, 190, 208.$$

The sum of the first 19 ones is 1990 and the difference between the 19th and the 20th is 18, so the sum is either 1990, or at least 2008, but never 1999.

17. Due to the lemma at the beginning of this chapter, all $n = 10^k - 1$ have the desired property. Let us prove that these are the only ones. Let

$$n = \overline{c_1 c_2 \ldots c_k}$$

Since n cannot be a power of 10, $10^{k-1} + 1 \leq n$, so

$$c_1 + c_2 + \ldots + c_k = S(n) = S\left(\left(10^{k-1} + 1\right) n\right)$$

$$= S\left(\overline{c_1 c_2 \ldots c_k} + c_1\right) + c_2 + \ldots + c_k \Rightarrow c_1 = S\left(\overline{c_1 c_2 \ldots c_k} + c_1\right) = S(n + c_1).$$

The first digit of $n + c_1$ will be c_1 (impossible) unless $c_1 = c_2 = \ldots = c_{k-1} = 9$. From $S(n) = S(2n)$, we deduce $c_k = 9$. Hence $n = 10^k - 1$.

18. (Titu Andreescu and Gabriel Dospinescu, USAMO 2005) We will prove that

$$\lfloor \lg(n+1) \rfloor \leq f(n) \leq 9 \lg \left\lceil \frac{n(n+1)}{2} + 1 \right\rceil,$$

which is enough to establish our claim. Let l be the smallest integer such that

$$10^l - 1 \geq \frac{n(n+1)}{2}.$$

Consider the set $X = \{j(10^l - 1) : 1 \leq j \leq n\}$. By the previous inequality and the statement about the digital sum of the multiples of numbers consisting only of 9s, it follows that

$$S\left(\sum_{x \in Y} x\right) = 9l$$

for all nonempty subsets Y of X, so $f(n) \leq 9l$ and the RHS is proved. Let m be the largest integer such that $n \geq 10^m - 1$. We will use the following well-known lemma:

Lemma. *Any set $M = \{a_1, a_2, \ldots, a_m\}$ has a nonempty subset whose sum of elements is divisible by m.*

Consider the sums a_1, $a_1 + a_2$,…, $a_1 + a_2 + \ldots + a_m$. If one of them is a multiple of m, then we are done. Otherwise, two of them congruent mod m, say the ith and the jth. Then $m \mid a_{i+1} + a_{i+2} + \ldots + a_j$ so we are done.

Hence, our set S has a subset whose sum of elements, N, is divisible by

$$10^m - 1 = 9 \cdot \underbrace{11 \ldots 11}_{m}.$$

Recall the lemma we used to solve problem 10. It follows that $S(N) \geq m$ and the LHS is also proved.

19. No, there isn't.
Suppose that we have $2^n = \overline{a_1 \dots a_k}$ and $2^m = \overline{a_{\alpha(1)} \dots a_{\alpha(k)}}$, with α a permutation of $1, \dots, k$. Assume that $2^m < 2^n$; because 2^m and 2^n both have k digits, we actually have $10^{k-1} \le 2^m < 2^n < 10^k$, implying that $2^{n-m} = 2^n/2^m < 10^k/10^{k-1} = 10$, therefore $n - m \le 3$.
On the other hand, we have $2^m \equiv S(2^m) = S(2^n) \equiv 2^n \pmod 9$, thus $2^{n-m} \equiv 1 \pmod 9$, which, evidently, is impossible for $1 \le n - m \le 3$. So, the answer is, indeed, negative.

20. We have, for positive integers k,
$$\frac{10^k - b}{a} = \frac{10^k + a - b}{a} - 1 < \left[\frac{10^k + a - b}{a}\right] \le \frac{10^k + a - b}{a},$$
implying that, for $n_k = [(10^k + a - b)/a]$, we have $10^k < an_k + b \le 10^k + a$; consequently, $10^k \le [an_k + b] \le 10^k + a$ for any k. This means that every integer part $[an_k + b]$ is equal to one of the (finitely many) natural numbers in the interval $[10^k, 10^k + a]$. Note that the sequence $(n_k)_{k \ge 1}$ is eventually strictly increasing. We conclude that there exists some j (that does not depend on k), with $0 \le j \le [a]$, and there are infinitely many values of k such that $[an_k + b] = 10^k + j$ for any of these ks (and the corresponding values of n_k are mutually distinct). Thus, for infinitely many (large enough) values of k we have $S([an_k + b]) = 1 + S(j)$, and this is what we intended to prove.

21. For numbers of the form $N = 2 \dots 21 \dots 1$ with k 2s and $2^k - 2k$ 1s, we have $S(N) = P(N) = 2^k$ (where $S(N)$ and $P(N)$ are respectively the sum and product of the digits of N). Such a number has $2^k - k$ digits, and the numbers $2^k - k$, $k \ge 1$, form a strictly increasing sequence. Therefore the statement from the problem is true for infinitely many n, namely for those of the form $n = 2^k - k$.

Further we show that the statement is false for numbers of the form $n = (2 \cdot 3 \cdot \ldots \cdot 9)^k$, with k a sufficiently large (we will see in the end *exactly how* large) natural number. Suppose that we have a natural number N with $n = (2 \cdot 3 \cdot \ldots \cdot 9)^k$ digits such that $S(N) = P(N)$, and suppose that N has precisely x_i digits equal to i, for $1 \le i \le 9$ (clearly, 0 cannot be a digit of such a number). Thus $S(N) = P(N)$ can be rewritten as
$$x_1 + 2x_2 + 3x_3 + \ldots + 9x_9 = 2^{x_2} \cdot 3^{x_3} \cdot \ldots \cdot 9^{x_9},$$
and, of course, we also have $x_1 + x_2 + \ldots + x_9 = n$, therefore,
$$n + x_2 + 2x_3 + \ldots + 8x_9 = 2^{x_2} \cdot 3^{x_3} \cdot \ldots \cdot 9^{x_9}.$$

From here, we conclude that $2^{x_2} \cdot 3^{x_3} \cdot \ldots \cdot 9^{x_9} \geq n = 2^k \cdot 3^k \cdot \ldots \cdot 9^k$, yielding that $x_i \geq k$ for at least one i from 2 to 9. This means that i^k divides $2^{x_2} \cdot 3^{x_3} \cdot \ldots \cdot 9^{x_9}$, and, because it also divides n, from the above equation, we obtain that i^k divides $x_2 + 2x_3 + \ldots + 8x_9$. Consequently,

$$2^k \leq i^k \leq x_2 + 2x_3 + \ldots + 8x_9 \leq 8(x_2 + x_3 + \ldots + x_9),$$

that is,

$$x_2 + \ldots + x_9 \geq 2^{k-3}.$$

On the other hand,

$$\begin{aligned} 9(2 \cdot 3 \ldots \cdot 9)^k &= 9n = 9(x_1 + x_2 + \ldots + x_9) \geq x_1 + 2x_2 + \ldots + 9x_9 \\ &= 2^{x_2} \cdot 3^{x_3} \cdot \ldots \cdot 9^{x_9} \geq 2^{x_2 + \ldots + x_9} \geq 2^{2^{k-3}}, \end{aligned}$$

and this represents a contradiction if it happens that we have

$$2^{2^{k-3}} > 9(2 \cdot 3 \cdot \ldots \cdot 9)^k.$$

And indeed, it happens because this is equivalent to

$$2^{k-3} > \log_2 9 + k \log_2(2 \cdot 3 \cdot \ldots \cdot 9)$$

and $\lim\limits_{k \to \infty} 2^{k-3}/k = \infty$, hence the inequality $2^{2^{k-3}} > 9(2 \cdot 3 \cdot \ldots \cdot 9)^k$ is true for all k starting from a threshold. This means that the hypothesis that there are numbers with n digits such that the sum and product of their digits are equal leads to a contradiction for all $n = (2 \cdot 3 \cdot \ldots \cdot 9)^k$, with k satisfying $2^{2^{k-3}} > 9(2 \cdot 3 \cdot \ldots \cdot 9)^k$, and the solution ends here.

22. The idea is that $d(N) = 3S(N) - S(3N)$, therefore

$$\begin{aligned} \sum_{n=1}^{m} \frac{d(3^n)}{3^n} &= \sum_{n=1}^{m} \frac{3S(3^n) - S(3^{n+1})}{3^n} = 3 \sum_{n=1}^{m} \left(\frac{S(3^n)}{3^n} - \frac{S(3^{n+1})}{3^{n+1}} \right) \\ &= 3 \left(\frac{S(3)}{3} - \frac{S(3^{m+1})}{3^{m+1}} \right). \end{aligned}$$

As $\lim\limits_{N \to \infty} S(N)/N = 0$, we have

$$\sum_{n=1}^{\infty} \frac{d(3^n)}{3^n} = \lim_{m \to \infty} 3 \left(\frac{S(3)}{3} - \frac{S(3^{m+1})}{3^{m+1}} \right) = S(3) = 3.$$

For proving $d(N) = 3S(N) - S(3N)$, let

$$N = \sum_{i=0}^{k-1} c_i 10^i,$$

where $c_i \in \{0, 1, \dots, 9\}$ are the decimal digits of N. For every $0 \le i \le k-1$, let $3c_i = 10a_i + b_i$, with $a_i = 0$ for $c_i \in \{0, 1, 2, 3\}$, $a_i = 1$ if $c_i \in \{4, 5, 6\}$, and $a_i = 2$ if $c_i \in \{7, 8, 9\}$, and with $b_i \in \{0, 1, \dots, 9\}$.

Evidently, we have $3s(N) = 10\sum_{i=0}^{k-1} a_i + \sum_{i=0}^{k-1} b_i$, and

$$\begin{aligned} 3N &= \sum_{i=0}^{k-1}(10a_i + b_i)10^i \\ &= a_{k-1}10^k + (a_{k-2} + b_{k-1})10^{k-1} + \dots + (a_0 + b_1)10 + b_0. \end{aligned}$$

If we have $a_{i-1} + b_i < 10$ for all $1 \le i \le k-1$, one can easily check the formula, since

$$3s(N) - s(3N) = 9\sum_{i=1}^{k-1} a_i = 9(a(N) + 2b(N)),$$

since $a_i = 1$ when $c_i \in \{4, 5, 6\}$ and $a_i = 2$ for $a_i \in \{7, 8, 9\}$. In this case, $c(N) = 0$. Indeed, one sees (after a careful, but quick examination) that the sequences (appearing in the decimal representation of N) of the form $3\dots3c$, with $c \ge 4$ and $3\dots36\dots6c$, with $c \ge 7$ are the only ones that can produce some $a_{i-1} + b_i$ at least equal to 10.

Because $3 \cdot \overline{3\dots3c} = \overline{10\dots0(3c-10)}$, when $c \in \{4, 5, 6\}$, the part of $3S(N) - S(3N)$ corresponding to such a sequence appearing in the decimal representation of N is $3(3p + c) - (3c - 9) = 9(p + 1)$, p being the number of 3s. Also, a sequence $3\dots3c$ with $c \in \{7, 8, 9\}$ contributes to $3S(N) - S(3N)$ with $3(3p + c) - (3c - 18) = 9(p + 2)$ (the product is now $3 \cdot \overline{3\dots3c} = \overline{10\dots01(3c-20)}$).

Finally, we have (for $c \in \{7, 8, 9\}$)

$$3 \cdot \overline{3\dots36\dots6c} = \overline{10\dots010\dots0(3c-20)},$$

hence the contribution of such a sequence to $3S(N) - S(3N)$ is

$$3(3p + 6q + c) - (3c - 18) = 9(p + 2q + 2),$$

where p is, like before, the number of 3s in the sequence, and q is the number of 6s. (We see that each digit of 6 has to be counted two times: once in $a(n)$, as being one of the digits $4, 5, 6$, and once in $c(n)$, as being part of the sequence.) Putting all these facts together, we have the proof of the formula $3S(N) - S(3N) = d(n)$, and the solution is complete.

For example,

$$3S(334591333668) - S(3 \cdot 334591333668) = 3 \cdot 54 - 27 = 135 = 9 \cdot 15$$
$$= 9(a(334591333668) + 2b(334591333668) + c(334591333668)).$$

23. a) For some positive integer k, we have

$$\sum_{n=1}^{km-1} \frac{[n/m]}{n(n+1)} = \sum_{j=1}^{k-1} \sum_{l=jm}^{(j+1)m-1} \frac{j}{l(l+1)} = \sum_{j=1}^{k-1} j \left(\frac{1}{jm} - \frac{1}{(j+1)m} \right)$$
$$= \sum_{j=1}^{k-1} \frac{1}{jm},$$

therefore

$$\sum_{n=1}^{km-1} \frac{n - m[n/m]}{n(n+1)} = \sum_{n=1}^{km-1} \frac{n}{n(n+1)} - m \sum_{n=1}^{km-1} \frac{[n/m]}{n(n+1)}$$
$$= \sum_{n=1}^{km-1} \frac{n}{n(n+1)} - \sum_{j=1}^{k-1} \frac{1}{j}$$

has limit $\ln m$ when k tends to infinity (in order to see that, just use the convergence of the sequence $(1 + 1/2 + \ldots + 1/n - \ln n)_{n \geq 1}$ to the Euler-Mascheroni constant, γ). The required result follows now by observing that $0 \leq n - m[n/m] < m$ for all n, which immediately leads to the conclusion that the sequence of partial sums is Cauchy.

b) We have

$$S_b(n) = n - (b-1) \sum_{k=1}^{\infty} \left[\frac{n}{b^k} \right] = (b-1) \sum_{k=1}^{\infty} \left(\frac{n}{b^k} - \left[\frac{n}{b^k} \right] \right)$$
$$= (b-1) \sum_{k=1}^{\infty} \frac{1}{b^k} \left(n - b^k \left[\frac{n}{b^k} \right] \right),$$

therefore

$$\sum_{n=1}^{\infty} \frac{S_b(n)}{n(n+1)} = (b-1) \sum_{n=1}^{\infty} \frac{1}{n(n+1)} \sum_{k=1}^{\infty} \frac{1}{b^k} \left(n - b^k \left[\frac{n}{b^k} \right] \right)$$
$$= (b-1) \sum_{k=1}^{\infty} \frac{1}{b^k} \sum_{n=1}^{\infty} \frac{n - b^k[n/b^k]}{n(n+1)} = (b-1) \sum_{k=1}^{\infty} \frac{1}{b^k} \ln(b^k)$$
$$= (b-1) \ln b \sum_{k=1}^{\infty} \frac{k}{b^k} = \frac{b}{b-1} \ln b.$$

Interchanging the order of summation is allowed, because the terms are positive. Then we used the result from the first part of the problem, and finally, we used

$$\sum_{k=1}^{\infty} kq^k = \lim_{K\to\infty} \sum_{k=1}^{K} kq^k = \lim_{K\to\infty} \frac{Kq^{K+2} - (K+1)q^{K+1} + q}{(1-q)^2} = \frac{q}{(1-q)^2},$$

for $|q| < 1$ (in our case, $q = 1/b$).

By the way, the relation

$$S_b(n) = n - (b-1)\sum_{k=1}^{\infty} \left[\frac{n}{b^k}\right]$$

(which is an easy exercise for the reader to prove) immediately proves one of the simplest properties of the sum of digits, namely $S_b(n) \equiv n \pmod{(b-1)}$. (In the case $b = 10$, mainly discussed by us, $S(n) \equiv n \pmod 9$.) Also, putting this together with $[x+y] \geq [x] + [y]$, one gets a simple proof for $S_b(m+n) \leq S_b(m) + S_b(n)$ for all positive integers m, n, and $b \geq 2$.

Chapter 5

Arithmetic and Geometric Progressions

Can you say in what way the following sequences are related

$$2,\ 5,\ 8,\ 11,\ 14,\ 17,\ 20,\ 23,\ 26,\ \ldots$$

$$3,\ 7,\ 11,\ 15,\ 19,\ 23,\ 27,\ 31,\ 35,\ \ldots\ ?$$

It can be easily seen that in both sequences, each term, starting with the second, is obtained from the previous term by adding the same constant (3, respectively 4). In general, a sequence of real numbers of the form

$$a,\ a+d,\ a+2d,\ \ldots\ ,\ a+nd,\ \ldots$$

is called an *arithmetic progression.* In some cases, the first term is denoted by a_1 and d is called the *(common) difference.* The general term of an arithmetic progression $(a_n)_{n\geq 1}$ is given by the formula

$$a_n = a_1 + (n-1)d, n \geq 1.$$

A sequence of real numbers of the form

$$b,\ bq,\ bq^2,\ \ldots,\ bq^n,\ \ldots$$

is called a *geometric progression.* In general, the first term is denoted by b_1 and q is called the *(common) ratio.* The general term of a geometric progression $(b_n)_{n\geq 1}$ is given by

$$b_n = b_1 q^{n-1}, n \geq 1.$$

Denote by S_n the sum of the first n terms of the progression,

$$S_n = b_1 + b_2 + \ldots + b_n.$$

We have

$$S_n = b_1 + b_1 q + \ldots + b_1 q^{n-1} = b_1(1 + q + \ldots + q^{n-1})$$

so, in case $q \neq 1$,

$$S_n = b_1 \frac{q^n - 1}{q - 1}, n \geq 1.$$

The reader might be confused because so far we have only considered *infinite* sequences when talking about arithmetic and geometric progressions. In fact, they may be very well finite — any finite subsequence of consecutive elements of an infinite arithmetic or geometric progression is a finite arithmetic or geometric progression. It is not hard to guess why they are called arithmetic and geometric progressions: because every member of the sequence is the arithmetic respectively geometric mean of its two neighbors. This way, we may also define *harmonic* progressions and sometimes even *quadratic* progressions.

Problem. Prove that if the real numbers a, b, and c form an arithmetic progression, then the same is true for the triples

(a) $a^2 - bc$, $b^2 - ac$, $c^2 - ab$;

(b) $b^2 + bc + c^2$, $a^2 + ac + c^2$, $a^2 + ab + b^2$.

Is the converse true?

Solution. Note that three numbers x, y, and z form an arithmetic progression if and only if $y - x = z - y \Leftrightarrow 2y = x + z$ (or we can say that y is the arithmetic mean of x and z). So, for part (a), we have to prove that if $2b = a + c$, then $2y = x + z$, with $x = a^2 - bc$, $y = b^2 - ac$, and $z = c^2 - ab$. But we have

$$\begin{aligned} x + z - 2y &= a^2 - bc + c^2 - ab - 2b^2 + 2ac \\ &= (a + c)^2 - 4b^2 - (ab + bc - 2b^2) \\ &= (a + c - 2b)(a + c + 2b) - (a + c - 2b)b \\ &= (a + c - 2b)(a + b + c), \end{aligned}$$

hence the implication $a + c - 2b = 0 \Rightarrow x + z - 2y = 0$ is clear. We also see that the reverse implication holds if we make the supplementary hypothesis that $a + b + c \neq 0$. Thus if a, b, and c are real numbers with nonzero sum, such that $x = a^2 - bc$, $y = b^2 - ac$, and $z = c^2 - ab$ form an arithmetic progression, then a, b, and c also form an arithmetic progression.

The reader will surely be able to handle part (b), which is actually very similar to part (a). Note that the above factorization of $x + z - 2y$ can be obtained by treating the expression $a^2 - bc + c^2 - ab - 2b^2 + 2ac$ as a second degree trinomial in, say, indeterminate a, and with b and c as parameters. Since the corresponding quadratic equation

$$a^2 - (b - 2c)a + c^2 - bc - 2b^2 = 0$$

has roots $2b-c$ and $-b-c$, the factorization of the trinomial follows.

Problem. Prove that there are infinitely many triples of perfect squares in arithmetic progression (that is, squares that are consecutive terms of an arithmetic progression).

Solution. We have the identity

$$(a^2-2ab-b^2)^2+(a^2+2ab-b^2)^2=2(a^2+b^2)^2$$

from which we see that, for any a and b (we will consider them integers) the squares $(a^2-2ab-b^2)^2$, $(a^2+b^2)^2$, and $(a^2+2ab-b^2)^2$ form an arithmetic progression. For instance, with $a=7$ and $b=4$, one gets the squares 23^2 $(=529)$, 65^2 $(=4225)$, and 89^2 $(=7921)$, which are in arithmetic progression.

Let us now consider some less trivial matters about arithmetic and geometric progressions. There are many hard questions in number theory and combinatorial number theory about arithmetic progressions. Let us now state some very important results about arithmetic progressions.

Dirichlet's Theorem. *For any pair of relatively prime positive integers a and d, the arithmetic progression $a+nd$ contains infinitely many prime numbers.*

The proof is quite difficult and not elementary. There are, however, elementary proofs for several particular cases such as $a=1$ or $a=-1$. This theorem is one of the greatest achievements in number theory and its proof is considered the act of birth of analytic number theory.

Related to arithmetic progressions containing prime numbers, it has recently been proved that the set of prime numbers contains arbitrarily long arithmetic progressions. This is one of the very few if not the only hard conjecture about the additive structure of prime numbers that has been proved.

Van der Waerden's Theorem. *For all positive integers k and r, there is a number N such that whenever the first N natural nonzero numbers are colored with r colors, there is a monochromatic arithmetic progression of length k. The smallest such number N is usually denoted $W(k,r)$.*

Unlike the previous one, this theorem is entirely elementary and not very hard to prove. Van der Waerden's theorem can also be formulated with an r-coloring of the set of positive integers instead of the first N positive integers, but it is not hard to see that these are equivalent. Probably many readers would like to know if every infinite set of positive upper density contains arbitrarily long arithmetic progressions because it is obvious that our theorem follows directly from this fact. Well, it is true, but much harder to prove than Van der Waerden's theorem. This is known as Szemeredi's theorem because he was the one to prove the cases $k=4$ and finally $k\geq 4$ after Roth gave an analytical proof of the case $k=3$.

Observe that Van der Waerden's theorem implies that if $\mathbb{N}=A\cup B$ where A and B are disjoint and A has no arithmetic progression with at least three terms, then B contains arbitrarily long arithmetic progressions. So, it is natural to ask whether it is true that B always contains an infinite arithmetic progression. The answer turns out to be negative.

Problem. Show that there exists a partition with two classes of the set of positive integers such that the first class contains no three numbers in arithmetic progression, while the second class contains no infinite arithmetic progression.

Solution. Observe that any infinite arithmetic progression of positive integers is determined by the first two terms, thus there are only countably many infinite arithmetic progressions of positive integers. Let $A_1, A_2, \ldots$ be an enumeration of them. It is immediate to construct by induction a sequence $(b_n)_{n\geq 1}$ such that $b_n \in A_n$ and $b_n + b_i \neq 2b_j$ for all $1 \leq i, j \leq n-1$ (essentially because A_n is infinite and the set of numbers of the form $2b_j - b_i$ with $1 \leq i, j \leq n-1$ is finite). Thus we can put in the first class the numbers $(b_n)_{n\geq 1}$ and in the second class all the other positive integers and we obtain a partition with the desired properties.

Very often it is useful to think of the infinite progression $(an+b)_{n\geq 1}$ as the set of positive integers satisfying $k \equiv b \pmod{a}$. This is obvious, but it makes life easier in many problems, including the following famous one, due to Pólya:

Problem. Show that in any infinite arithmetic progression of integers, there are infinitely many terms having precisely the same set of prime divisors.

Solution. Let $(an+b)_{n\geq 1}$ be this progression and let $d = \gcd(a, b)$. Write $a = du$, $b = dv$ with $\gcd(u, v) = 1$. Clearly, it is enough to prove the same result for the progression $(un+v)_{n\geq 1}$, that is to find infinitely many numbers $k \equiv v \pmod{u}$, all having the same prime divisors. This is not difficult, because if $v \neq 1$, one can consider $k = v^{1+s\varphi(u)}$ for $s \geq 1$, while if $v = 1$, we can take $k = (1+u)^s$ for $s \geq 1$.

The same idea is used in the more challenging problem that follows.

Problem. Let $(a_n)_{n\geq 1}$ be an infinite arithmetic progression of positive integers. Prove that the sequence

$$\frac{1}{a_1}, \frac{1}{a_2}, \frac{1}{a_3}, \frac{1}{a_4}, \ldots$$

contains arbitrarily long arithmetic progressions.

Solution. Let $a_n = an + b$. We may clearly assume that $\gcd(a, b) = 1$. Let us search for an arithmetic progression of length N of the form

$$\frac{a+b}{(a+b)(2a+b)\ldots(Na+b)}, \frac{2a+b}{(a+b)\ldots(Na+b)}, \ldots, \frac{Na+b}{(a+b)\ldots(Na+b)}.$$

Now, we try to find N such that $\frac{1}{ja+b}\prod_{i=1}^{N}(ai+b)$ is a term of $(a_n)_{n\geq 1}$ for all

$1 \leq j \leq N$. This comes down to

$$\prod_{1 \leq i \neq j \leq N} (ai+b) \equiv b \pmod{a}.$$

But $\prod\limits_{1 \leq i \neq j \leq N} (ai+b) \equiv b^{N-1} \equiv b \pmod{a}$ if $N \equiv 2 \pmod{\varphi(a)}$. Because there are infinitely many N satisfying the last condition, the problem is solved.

We end this theoretical part with a beautiful problem given in the Romanian Team Selection Test in 1999.

Problem. Prove that for all $n \geq 3$, there are n positive integers $a_1, a_2, \ldots, a_n$ in arithmetic progression and n positive integers $b_1, b_2, \ldots, b_n$ in geometric progression such that

$$b_1 < a_1 < b_2 < a_2 < \ldots < b_n < a_n.$$

Solution. Define $B_k = \left(1 + \frac{1}{m}\right)^k$ and observe that for $k \geq 2$, we have

$$B_k > 1 + \frac{k}{m}.$$

Also, for $k \leq n$,

$$B_k \leq 1 + \frac{k}{m} + \left[\frac{n(n-1)}{m} \cdot 12! + \frac{n(n-1)(n-2)}{m^2} \cdot \frac{1}{3!} + \ldots + \right.$$
$$\left. + \frac{n(n-1)\ldots(n-k+1)}{m^{k-1}} \cdot \frac{1}{k!}\right] \frac{1}{m}.$$

Thus, if $m > n^2$, we have

$$B_k < 1 + \frac{k}{m} + \frac{1}{m} = 1 + \frac{k+1}{m}.$$

Define then $A_k = 1 + \frac{k+1}{m}$ for $1 \leq k \leq n$; then the previous remarks show that

$$B_1 < A_1 < B_2 < A_2 < \ldots < B_n < A_n.$$

It is now enough to consider $a_k = m^n A_k$, $b_k = m^n B_k$.

Proposed Problems

1. Let a, b, and c be real numbers such that $a+b$, $a+c$ and $b+c$ are nonzero, and such that a^2, b^2, and c^2 form an arithmetic progression. Prove that
$$\frac{a}{b+c}, \frac{b}{a+c}, \frac{c}{a+b}$$
also form an arithmetic progression. Is the converse true?

2. Prove that the nonzero real numbers $x_0, x_1, \ldots, x_n$ form a (finite) geometric progression if and only if

$$(x_0^2 + \cdots + x_{n-1}^2)(x_1^2 + \cdots + x_n^2) = (x_0 x_1 + \cdots + x_{n-1} x_n)^2.$$

3. Prove that the nonzero real numbers a, b, c form (in a certain order) a geometric progression if and only if

$$abc(a^3 + b^3 + c^3) = a^3 b^3 + a^3 c^3 + b^3 c^3.$$

4. Let $(a_n)_{n \geq 1}$ be an arithmetic progression and let $(b_n)_{n \geq 1}$ be a geometric progression, both with positive terms, and such that $a_1 = b_1$, and $a_2 = b_2$. Prove that $a_n \leq b_n$ for all $n \geq 1$.

5. Prove that the numbers $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{5}$ do not belong to the same arithmetic progression.

6. Prove that n distinct real numbers form an arithmetic progression if and only if the number of different distances between them is $n - 1$.

7. Prove that if the prime numbers $p_1 < p_2 < \ldots < p_{12}$, $p_1 \geq 13$ form an arithmetic progression of difference d, then $d > 2000$.

8. Are there sets $A \subset \mathbb{N}$ which contain arbitrarily long arithmetic progressions but do not contain infinite arithmetic progressions?

9. Prove that in every infinite arithmetic progression of positive integers a number exists whose decimal representation contains the digit 9.

10. Let $a_1, a_2, \ldots, a_n$ be an arithmetic progression such that i divides a_i for all $i \in \{1, 2, \ldots, n-1\}$, but n does not divide a_n. Prove that $n = p^t$ for a prime number p and a positive integer t.

11. Are there (a) arbitrarily long, (b) infinite arithmetic progressions, all of their terms having the same sum of digits?

12. Prove that no matter how the set of positive integers is partitioned into finitely many arithmetic progressions, one of them has the property that its first term is divisible by its common difference. Also prove that the sum of the reciprocals of the common differences of these progressions equals 1.

13. Each of the points of a circle is colored in one of three colors. Prove that there is a monochromatic isosceles triangle with all vertices on the circle.

14. Let $A \subset \mathbb{R}^+$, $|A| = n$, $n \geq 4$ with the property that $a, b \in A$, $a > b$ implies $a + b \in A$ or $a - b \in A$. Prove that the elements of A form an arithmetic progression.

15. Prove that there is a set $A \subset \{1, 2, \ldots, 40\}$ with 16 elements which does not contain 3 elements in arithmetic progression.

16. Prove that any arithmetic progression $np^k + 1$, $n \in \mathbb{N}$, where p is an odd prime and $k \geq 1$ contains infinitely many prime numbers.

17. Let n be an integer with $n \geq 7$. Let $1 = a_1 < a_2 < \ldots < a_k = n - 1$ be all positive integers less than n and relatively prime to n. If $a_1, a_2, \ldots, a_k$ form an arithmetic progression, prove that n is either prime or a power of 2.

18. Consider the sequence $a_n = 3^n - 2^n$. Prove that the sequence does not contain three terms in geometric progression.

19. We say that a positive integer n is a *power* if there are $t, s \in \mathbb{Z}$, $t, s \geq 2$ such that $n = t^s$. Are there (a) arbitrarily long, (b) infinite arithmetic progressions, all of their terms being powers?

20. Let $(b_n)_{n\geq 1}$ be an infinite increasing geometric progression, with nonzero terms. Show that there exists an arithmetic progression $(a_n)_{n\geq 1}$ such that $(b_n)_{n\geq 1}$ is a subsequence of $(a_n)_{n\geq 1}$ if and only if the common ratio of $(b_n)_{n\geq 1}$ is a positive integer greater than 1.

21. Prove that if an infinite arithmetic sequence of nonnegative integers contains a perfect square and a perfect cube, then it also contains a sixth power of some natural number.

Solutions

1. Find a way (there are many) to prove the identity

$$\frac{a}{b+c} + \frac{c}{a+b} - 2\frac{b}{a+c} = \frac{(a+b+c)(a^2+c^2-2b^2)}{(a+b)(a+c)(b+c)}$$

and the conclusion follows. Note that the converse is true if $a+b+c \neq 0$.

2. This is nothing but the equality case in Cauchy-Schwarz's inequality. Namely, we have (for real numbers $a_1, \ldots, a_n, b_1, \ldots, b_n$)

$$(a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2) \geq (a_1b_1 + \cdots + a_nb_n)^2$$

and the equality

$$(a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2) = (a_1b_1 + \cdots + a_nb_n)^2$$

holds if and only if $a_1, \ldots, a_n$ are proportional to $b_1, \ldots, b_n$ respectively; that is, if and only if

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} = \cdots = \frac{a_n}{b_n}$$

(if $b_1, \ldots, b_n$ are nonzero). In our problem, the equality

$$(x_0^2 + \cdots + x_{n-1}^2)(x_1^2 + \cdots + x_n^2) = (x_0x_1 + \cdots + x_{n-1}x_n)^2$$

is therefore equivalent to

$$\frac{x_1}{x_0} = \frac{x_2}{x_1} = \cdots = \frac{x_n}{x_{n-1}},$$

which means that $x_0, x_1, \ldots, x_n$ form a geometric sequence.

3. Indeed, we have

$$abc(a^3 + b^3 + c^3) - (a^3b^3 + a^3c^3 + b^3c^3) = (a^2 - bc)(b^2 - ac)(c^2 - ab),$$

hence the equality from the problem statement is equivalent to either $a^2 = bc$, or $b^2 = ac$, or $c^2 = ab$. But $a^2 = bc$ means $a/b = c/a$ (that is, b, a, c is a three-term geometric progression), and so on.

4. The inequality to prove is

$$a_1 + (n-1)d \le b_1r^{n-1}$$

where $d = a_2 - a_1$ is the common difference of the arithmetic progression, and $r = b_2/b_1$ is the common ratio of the geometric progression. Thus we want to show that

$$a_1 + (n-1)(a_2 - a_1) \le b_1\left(\frac{b_2}{b_1}\right)^{n-1} \Leftrightarrow 1 + (n-1)(x-1) \le x^{n-1}$$

for $x = a_2/a_1 = b_2/b_1 > 0$ and every positive integer n. This is just one of the many forms of Bernoulli's inequality, and it arises, for example, from the identity

$$x^{n-1} - 1 - (n-1)(x-1) = (x-1)^2(x^{n-3} + 2x^{n-4} + \cdots + (n-3)x + n - 2).$$

5. Suppose, by way of contradiction, that there are a and r such that $\sqrt{2} = ak + r$, $\sqrt{3} = al + r$, $\sqrt{5} = am + r$. Hence,

$$\frac{\sqrt{5}-\sqrt{2}}{\sqrt{5}-\sqrt{3}} = \frac{m-k}{m-l} \in \mathbb{Q},$$

a contradiction. Indeed, by squaring, we obtain a relation of the form $\sqrt{10} = x + y\sqrt{15}$ with $x, y \in \mathbb{Q}$. By squaring again and taking into account that $\sqrt{10}, \sqrt{15} \notin \mathbb{Q}$, we easily conclude the desired result.

6. The direct implication is trivial. Now suppose $a_1 < a_2 < \ldots < a_n$ are n numbers with that property. Because $a_n - a_1 > a_n - a_2 > \ldots > a_n - a_{n-1}$, we already have $n-1$ possible differences. Since $a_{n-1} - a_1 > a_{n-1} - a_2 > \ldots > a_{n-1} - a_{n-2}$ and they are all strictly smaller than $a_n - a_1$, it follows that $a_{n-1} - a_{k-1} = a_n - a_k$, or $a_k - a_{k-1} = a_n - a_{n-1} =$ constant, hence our sequence is an arithmetic progression.

7. Take a prime $q < 12$. If q does not divide d, $p_1, p_2, \ldots, p_q$ have different remainders when divided by q, hence at least one of them is divisible by q. But all of them are primes greater than q, which is a contradiction. Hence

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310 \mid d,$$

so $d > 2000$.

8. Yes, there are. One example is the set of positive integers with an odd number of digits. It is clear that this set contains arbitrarily long arithmetic progressions because it has arbitrarily long blocks of consecutive numbers. On the other hand, it has arbitrarily long gaps, hence it cannot contain infinite arithmetic progressions because such sequences cannot "leap" over gaps larger than their common difference.

   You can find two more examples in problems 11 and 19 below.

9. Let r be the ratio, let a be the first term, and let d be such that $10^{d-1} > \max\{r, a\}$. If b is the largest term of the progression not exceeding 10^d, then it is clear that its first digit is 9.

   A much more challenging question is the following: what is the largest possible length of a finite arithmetic progression which does not contain such numbers? The answer is 72, but the problem is hard.

10. (Baltic Way 2000) Let $a_k = u + dk$. Suppose, by way of contradiction, that n is not a prime power. Then there are $a, b < n$, relatively prime, with $n = ab$. Due to the hypothesis, $a \mid u + ak \Rightarrow a \mid u$ and $b \mid u + bk \Rightarrow b \mid u$, so $n = ab \mid u \Rightarrow n \mid u + an$, false, i.e., n is a prime power.

11. There are no infinite arithmetic progressions with this property. Since the difference between two consecutive terms is constant (hence bounded), any infinite arithmetic progression contains numbers which begin with arbitrarily many 9s. Therefore, there are numbers with arbitrarily large sum of digits, a contradiction. The answer for the other question is positive. The key is that $S((10^k - 1)N) = 9k$ for all $N \leq 10^k - 1$. Let $N = \overline{a_1a_2\ldots a_k}$. Now we have

$$(10^k - 1)N = 10^kN - N = \overline{a_1a_2\ldots a_k00\ldots00} - \overline{a_1a_2\ldots a_k}$$

$$= \overline{a_1a_2\ldots(a_k - 1)(9 - a_1)(9 - a_2)\ldots(9 - a_{k-1})(10 - a_k)},$$

so $S((10^k - 1)N) = 9k$ for all $N \leq 10^k - 1$, and the proof is complete.

12. Let $\{a_i + kd_i,\ k \in \mathbb{N}\}$, $i = 1, \ldots, n$ be the n arithmetic progressions. Due to the hypothesis, there is an $i \in \{1, 2, \ldots, n\}$ with

$$a_i + kd_i = d_1d_2\ldots d_n \Rightarrow d_i \mid a_i$$

hence the first part of our problem is solved.

For the second part, note that the set of positive integers at most equal to N can be written as the disjoint union of n sets; set i consists of the integers from $\{1, \ldots, N\}$ that also belong to progression $\mathcal{P}_i = \{a_i + kd_i : k = 0, 1, \ldots\}$:

$$\{1, \ldots, N\} = \bigcup_{i=1}^{n} (\{1, \ldots, N\} \cap \mathcal{P}_i).$$

The equality of the cardinalities of these sets reads

$$N = \sum_{i=1}^{n} \left(\left[\frac{N - a_i}{d_i} \right] + 1 \right).$$

If we divide by N and pass to the limit for $N \to \infty$, we get the desired equality

$$1 = \sum_{i=1}^{n} \frac{1}{d_i}.$$

Alternatively, one can avoid the passage to the limit, if one observes that among any d_i consecutive positive integers, there is exactly one term belonging to progression $\mathcal{P}_i$. Consequently, if we choose $N = d_1 \cdots d_n$, then among the first N positive integers, there exist precisely N/d_i terms of the progression $\mathcal{P}_i$, hence the equality of the cardinalities of the above sets becomes $N = \sum_{i=1}^{n} N/d_i$, which is the required relation.

The reader will agree (try this as an exercise!) that, starting from

$$\sum_{i=1}^{n}\left(\sum_{x\in\{1,\ldots,N\}\cap\mathcal{P}_i} x\right)=1+\cdots+N$$

and after performing some computations, one can obtain

$$\sum_{i=1}^{n}\frac{a_i}{d_i}=\frac{n+1}{2}.$$

Such partitions of the set of positive integers are called *covers*. Covers are an important research source in number theory. Interested readers are encouraged to read and find out more about them.

13. Consider $W(3,3)$ equally distanced points on this circle. By Van der Waerden's Theorem, there are three which determine an isosceles triangle.

14. Let $0 < a_1 < a_2 < \ldots < a_n$ be the elements of A.

    Since $a_n+a_k > a_n$, $a_n-a_k \in A$, hence $a_n-a_k = a_{n-k}$, or $a_k+a_{n-k} = a_n$, $k = 1,2,\ldots,n-1$. For $2 \le k \le n-2$, $a_k + a_{n-1} > a_1 + a_{n-1} = a_n$, hence $a_{n-1}-a_k \in A$, but $a_{n-1}-a_k \le a_{n-1}-a_2 < a_n - a_2 = a_{n-2}$, hence $a_{n-1} - a_k = a_{n-k-1}$. We deduce that $a_k - a_{k-1} = a_n - a_{n-1}$ for $k \ge 3$, hence $a_2, a_3, \ldots, a_n$ form an arithmetic progression. Now it is easy to see that the whole sequence is an arithmetic progression.

15. Choose A to be the set of all positive integers in that range which contain only 1 and 0 in their base-3 representation. It is easy to see that this set has the desired property.

16. This is a special case of Dirichlet's theorem. We will prove that for every integer n, there is a prime q such that $q \equiv 1 \pmod{p^n}$. Using this fact for $n = k, k+1, \ldots$ successively, we get that the equation $x \equiv 1 \pmod{p^k}$ has infinitely many solutions in prime numbers. We begin with a well-known result:

    Lemma. *If $a \ge 2$, then there is a prime q such that $q \mid a^p - 1$, but q does not divide $a-1$.*

    Proof. Let q be a prime such that

    $$q \mid A = 1 + a + a^2 + \ldots + a^{p-1} = \frac{a^p-1}{a-1}.$$

    Clearly, $q \mid a^p - 1$. If $q \mid a - 1 \Leftrightarrow a \equiv 1 \pmod{q}$, we have

    $$0 \equiv 1 + a + a^2 + \ldots + a^{p-1} \equiv p \pmod{q},$$

so $q = p$. Consequently, two possibilities arise: either $A = p^m$ for some positive integer m, or A has a prime divisor $q \neq p$, for which q divides $a^p - 1$ and q does not divide $a - 1$.

Assume $A = p^m$ has no prime divisor different from p. Let $a - 1 = p^u v$, $(v, p) = 1$. Then,

$$p^{m+u}v = (p^u v + 1)^p - 1 = \sum_{i=0}^{p} \binom{p}{i} p^{iu} v^i - 1 = \sum_{i=1}^{p} \binom{p}{i} p^{iu} v^i,$$

hence the exponent of p in the factorization of $p^{m+u}v$ is actually $u + 1$, meaning that $m = 1$, and $A = p$ — which is impossible for $a \geq 2$. (Note that here we use the fact that p is odd.) Thus there must exist a prime divisor q of A different from p, for which q divides $a^p - 1$ and q does not divide $a - 1$.

Due to the lemma, there is a prime number q such that $q \mid 2^{p^n} - 1$, but q does not divide $2^{p^{n-1}} - 1$. From $q \mid 2^{p^n} - 1$ and Fermat's theorem (according to which $q \mid 2^{q-1} - 1$), it follows that $q \mid 2^{(p^n, q-1)} - 1$. But this shows that $q \equiv 1 \pmod{p^n}$, because otherwise,

$$(p^n, q-1) \mid p^{n-1} \Rightarrow 2^{(p^n, q-1)} - 1 \mid 2^{p^{n-1}} - 1 \Rightarrow q \mid 2^{p^{n-1}} - 1,$$

which is not true.

Observe however that everything we said in the last paragraph works for $p = 2$, too — except for the words "due to the lemma". Thus the result can be proved by this method also for $p = 2$, when we do not need the lemma (which is not true in this case, for example if we take $a = 2^s - 1$).

17. (Laurenţiu Panaitopol, IMO 1991) Let d be the common difference of the progression. If n is odd, let $n = 2l + 1$. Then $(l, n) = 1$ and $(l+1, n) = 1$, so there is $t \in \{1, 2, \ldots, k - 1\}$ such that $a_{t+1} - a_t = 1$. That is, $d = 1$, and all numbers smaller than n are relatively prime to it, hence n is a prime number.

    Let us consider now the case when n is even. Let $n = 2^\alpha \beta$ with $\alpha \geq 1$, and $\beta \equiv 1 \pmod 2$. Note that $(\beta+2, n) = 1$ and $(\beta+4, n) = 1$ since 2 and 4 are powers of 2. In fact, if $p \mid \beta + 2^m$ and $p \mid n$ with p prime, p cannot be 2 since $\beta + 2^m$ is odd, and if p is odd, $p \mid n \Rightarrow p \mid \beta$, so $p \mid 2^m$, which is false. Moreover, $n = 2^\alpha \beta \geq 2\beta$ and $n \geq 8$ imply $\beta \leq n/2 \leq n - 4$, so there are s and t such that $a_s = \beta + 2$ and $a_t = \beta + 4$. Thus $a_t - a_s = 2$, and $d \mid 2$. Since n is even and greater than 2, n is not a prime and $d \neq 1$ follows, hence $d = 2$, meaning that $a_i = 2i - 1$ for all $i \in \{1, 2, \ldots, k\}$; therefore n has no odd divisor except for 1 (and it is even), so n is a power of 2.

18. **Solution I.** (Laurenţiu Panaitopol) It is clear that the sequence is strictly increasing.

Lemma. *If* $m < n$, *then the following double inequality holds:*

$$a_m a_{2n-m} < a_n^2 < a_m a_{2n-m+1}.$$

Proof. The first inequality is equivalent to

$$\left(3^m - 2^m\right)\left(3^{2n-m} - 2^{2n-m}\right) < \left(3^n - 2^n\right)^2 \Leftrightarrow \left(3^{n-m} - 2^{n-m}\right)^2 > 0,$$

which is true. The second one can be rewritten as

$$\begin{aligned}&\left(3^{m-1} - 2^{m-1}\right)\left(2 \cdot 3^{2n-m+1} - 2^{2n-m+1}\right)\\ &= 2 \cdot 2^n \cdot 3^{m-1}\left(3^{n-m+1} - 2^{n-m+1}\right) > 0\end{aligned}$$

and this is true as well, so the lemma is proved.

Suppose, by way of contradiction, that there are $m, n, p \in \mathbb{Z}^+$ such that $a_n^2 = a_m a_p$. But from our lemma,

$$2n - m < p < 2n - m + 1,$$

which is a contradiction, and the problem is solved.

Solution II. It is well-known that a_n is a Mersenne sequence, i.e., $a_{(m,n)} = (a_m, a_n)$. Suppose, by way of contradiction, that a_n has three different terms in geometric progression.

Lemma. *Let* n *be the smallest positive integer for which there are* m, p, $m < n < p$ *such that* a_m, a_n, a_p *is a geometric progression. Then* $m \mid n \mid p$.

Proof. If a, b, c are integers such that $b^2 = ac$, then $(b, a)^2 = a(a, c)$. Using this for a_m, a_n, a_p and keeping in mind the fact that a_n is a Mersenne sequence, it follows that

$$a_{(m,n)}^2 = a_m a_{(m,p)} \text{ and } a_{(n,p)}^2 = a_p a_{(m,p)}.$$

Let us look at the first equation. From the minimality of n, it follows that $(m, n) = n$ or $(m, n) = m = (m, p)$ hence $m \mid n$ or $n \mid m$ and since $m < n$, it follows that $m \mid n$. Analogously, $n \mid p$ from the second equation. In conclusion, $m \mid n \mid p$.

Let $n = m\alpha$ and $p = n\beta$, $\alpha, \beta \geq 2$. Then we have

$$a_{\alpha n}^2 = a_n a_{\alpha\beta n} \geq a_1 a_{2\alpha n} > a_{\alpha n}^2$$

since $a_{2n} > a_n^2 a_1$.

19. The answer to the first question is positive, while to the second one the answer is negative. Let us first solve (a). Let n be a positive integer. Let $2 = p_1 < p_2 < \ldots < p_k \leq n$ be all prime numbers not exceeding n. Let $2 \leq a_1 < a_2 < a_3 < \ldots < a_n$ be n pairwise relatively prime positive integers. We will prove that there is a positive integer d such that $d, 2d, 3d, \ldots, nd$ are all powers. We will search for a d of the form

$$d = \prod_{i=1}^{k} p_i^{\alpha_i}, \alpha_i \in \mathbb{N}$$

For all $j \in \{1, 2, \ldots, n\}$, let $j = \prod_{i=1}^{k} p_i^{\alpha_i(j)}$. Due to the Chinese Remainder Theorem, for all $i \in \{1, 2, \ldots, k\}$, there is $\alpha_i \in \mathbb{N}$ such that

$$\alpha_i \equiv -\alpha_i(j) \pmod{a_j}, \ j = 1, \ldots, n.$$

Let us now choose

$$d = \prod_{i=1}^{k} p_i^{\alpha_i}$$

and observe that jd is a power of exponent a_j since

$$a_j \mid \alpha_i + \alpha_i(j) = \exp_{p_i}(dj), \ i = 1, 2, \ldots, k$$

Let us now solve (b). Suppose, by way of contradiction, that there are $a, d \in \mathbb{N}$ such that $a + dn$ is a power for every $n \in \mathbb{N}$. Let $p > d$ be a prime number. Since $(d, p^2) = 1$, there is $n \in \mathbb{N}$ such that

$$dn \equiv p - a \pmod{p^2} \Rightarrow a + dn \equiv p \pmod{p^2} \Rightarrow \exp_p(a + dn) = 1$$

which shows that $a + dn$ cannot be a power, a contradiction. Another way to solve (b) is to prove that the set of powers has density 0, hence it cannot contain an infinite arithmetic progression, which has positive density.

20. Suppose $b_n = br^n$ with b and r nonzero real numbers, $b \neq 0$ and that the geometric sequence $(b_n)_{n \geq 1}$ is a subsequence of the arithmetic progression $(a_n)_{n \geq 1}$, where $a_n = a + nd$ for all $n \geq 0$, with a and d real numbers. Thus we have

$$br^k = a + n_k d$$

where n_k are nonnegative integers for all $k \in \mathbb{N}$. It follows that

$$(n_{k+1} - n_k)d = br^k(r - 1)$$

for all k and, by dividing side by side two consecutive equalities of this type, we get

$$r = \frac{n_{k+2} - n_{k+1}}{n_{k+1} - n_k},$$

for every $k \geq 0$. We conclude, in the first place, that r is a rational number, and, second, multiplying these equalities for k from 0 to $p-1$ yields

$$n_{p+1} - n_p = r^p(n_1 - n_0)$$

for all $p \geq 0$. (Thus we obtained that the sequence with general term $n_{k+1} - n_k$ is a geometric progression with common ratio r.)

Suppose $r = s/t$ with relatively prime positive integers s and t. The above equality reads

$$t^p(n_{p+1} - n_p) = s^p(n_1 - n_0),$$

and, consequently, it shows that t^p is a divisor of $n_1 - n_0$ for every nonnegative integer p (because s^p and t^p are relatively prime). Of course, this can happen only if $t = 1$, leading to the fact that $r = s$ is a natural number (greater than 1, by hypothesis).

Conversely, if $b_n = br^n$, with positive integer r, it is clear that the geometric progression $(b_n)_{n\geq 1}$ (with common ratio r) is a subsequence of the arithmetic progression with general term bn. This problem was proposed by Mihai Bălună, for a training camp test (very) many years ago.

21. Let $(a + nd)_{n\geq 0}$ be an arithmetic progression with the first term a and the common difference d, a nonnegative integer (if d was negative, then $a + nd$ would also be negative for large enough n) that has two terms $a + kd = x^2$ and $a + ld = y^3$ a square and a cube, respectively. We intend to prove that there also exist nonnegative integers s and z such that $a + sd = z^6$.

    Note first that, even in the case when the progression is constant (when $d = 0$), the problem is not entirely trivial. Basically, in this case, we need to show that if a natural number is both a square and a cube, then it is also a sixth power of some natural number. After a moment of thinking, the reader will realize that this is a consequence of the unique factorization theorem (except for the numbers 0 and 1, for which there is nothing to prove). We consider further that $d \geq 1$.

    Let $\delta = (a, d)$ be the greatest common divisor of a and d, and let $a = \delta a_1$, $d = \delta d_1$, with a_1 and d_1 relatively prime positive integers (actually a_1 can be 0). Observe that if π is a prime common factor of δ and d_1, then it cannot be a divisor of $a_1 + kd_1$ or of $a_1 + ld_1$ (for otherwise, it would be a common divisor of a_1 and d_1). Thus, using the equalities $x^2 = \delta(a_1 + kd_1)$ and $y^3 = \delta(a_1 + ld_1)$ and the unique factorization theorem, we conclude that the exponent of π in the prime factorization of δ is a multiple of 2, and a multiple of 3, too — hence it is divisible by 6. It follows that δ can be written in the form $\delta = \alpha^6\beta$, with positive integers α and β. Here, α is the product of all prime factors like π, that is, the common factors of δ and d_1 (and each such factor has, in the factorization of δ, an exponent divisible by 6), while β consists of those prime factors of δ that are *not* factors of d_1, therefore β and d_1 are relatively prime. Of course α, β (or both) could be empty products (that is, equal to 1). Now it is well-known (and it is not hard to see; use again the unique factorization theorem) that if u^k divides v^k, for integers u and v, and positive integer k, then u also divides v. In our case, because $\alpha^6 = (\alpha^3)^2$ divides x^2, it follows that $x_1 = x/\alpha^3$ is a natural number, and $x_1^2 = \beta(a_1 + kd_1)$; similarly, $y_1 = y/\alpha^2$ is a natural number, and $y_1^3 = \beta(a_1 + ld_1)$.

Now view the equalities $x_1^2 = \beta(a_1 + kd_1)$ and $y_1^3 = \beta(a_1 + ld_1)$ as equalities in the ring $\mathbb{Z}/d_1\mathbb{Z}$ of the residue classes modulo d_1 (but, for the sake of simplicity of notations, we allow the elements of the quotient ring to be named like the corresponding ones from $\mathbb{Z}$). They appear to be $x_1^2 = \beta a_1$, and $y_1^3 = \beta a_1$. Because each of a_1 and β is relatively prime to d_1 (as numbers), we conclude that βa_1 is invertible in $\mathbb{Z}/d_1\mathbb{Z}$, yielding that x_1 and y_1 are invertible, too. Raise the equalities $x_1^2 = \beta a_1$ and $y_1^3 = \beta a_1$ to powers with exponents 3 and -2 respectively, then multiply the equalities thus obtained (in $\mathbb{Z}/d_1\mathbb{Z}$) in order to obtain

$$(x_1 y_1^{-1})^6 = \beta a_1, \quad \text{or} \quad (x_1 y_1^{-1}\beta^{-1})^6\beta^5 = a_1,$$

y_1^{-1} and β^{-1} being the inverses of y_1 and β respectively, regarded as elements (of the multiplicative group of invertible elements) of $\mathbb{Z}/d_1\mathbb{Z}$. Now there is a natural number w such that $x_1 y_1^{-1}\beta^{-1} = w$ in $\mathbb{Z}/d_1\mathbb{Z}$, hence the above equality can also be written in the form $w^6\beta^5 = a_1$ (in $\mathbb{Z}/d_1\mathbb{Z}$) which yields an equality of the form $\beta^5 w^6 = a_1 + sd_1$ (in $\mathbb{Z}$), for some nonnegative integer s. Finally this implies

$$z^6 = \alpha^6\beta(a_1 + sd_1) = \delta(a_1 + sd_1) = a + sd \quad \text{for} \quad z = \alpha\beta w,$$

finishing the proof.

The reader will surely be able to prove in the same manner the general fact that if an arithmetic progression contains an mth power (that is, a power of a natural number with exponent m), and it contains an nth power, then it also has a term that is a $[m, n]$th power (where $[m, n]$ is the least common multiple of positive integers m and n).

Chapter 6

Complementary Sequences

Let a_0, a_1, $a_2, \ldots$ be an increasing sequence of nonnegative integers. We can define the increasing sequence b_0, b_1, $b_2, \ldots$ of nonnegative integers such that

$$(\{a_n \mid n \in \mathbb{N}\}\ ,\ \{b_n \mid n \in \mathbb{N}\})$$

is a partition of $\mathbb{N}$. The sequence $(b_n)_{n\in\mathbb{N}}$ is called *the complementary sequence* of the sequence $(a_n)_{n\in\mathbb{N}}$. For example, the complementary sequence of nonnegative even integers $0, 2, 4, 6, 8, 10, 12, \ldots$ is the sequence of positive odd integers $1, 3, 5, 7, 9, 11, 13, 15, \ldots$.

We can find the general term of the complementary sequence $(b_n)_{n\in\mathbb{N}}$ in terms of $(a_n)_{n\in\mathbb{N}}$ by the following:

Proposition 1. *For each $n, k \in \mathbb{N}$, the following implication holds*

$$n \in \mathbb{N} \cap [a_k - k, a_{k+1} - (k+1)) \Rightarrow b_n = n + k + 1. \tag{1}$$

Proof. Let $k \in \mathbb{N}$. The sequence $(b_n)_{n\in\mathbb{N}}$ must take each value between a_k, a_{k+1} consecutively. Then

$$b_{m+1} - b_m = 1, \tag{2}$$

for all $m \in \mathbb{N}$ such that $a_k < b_m < b_{m+1} < a_{k+1}$.

Now let us find m such that $a_k < b_m < a_{k+1}$. Let m be the smallest integer for which $a_k < b_m$. Then if $a_{k+1} - a_k \geq 2$,

$$b_m = a_k + 1. \tag{3}$$

There are $k+1$ terms $a_0, a_1, \ldots, a_k$ of $(a_n)_{n\in\mathbb{N}}$ which are less than b_m. The rest of

$$a_k + 1 - (k+1) = a_k - k$$

are elements of $(b_n)_{n\in\mathbb{N}}$: $b_0, b_1, \ldots, b_{a_k-k-1}$. Hence $m = a_k - k$, and from (3), we have

$$b_{a_k - k} = a_k + 1 \Rightarrow b_m = m + k + 1.$$

Now the conclusion follows from (2).

Proposition 2. *Let* $(a_n)_{n\in\mathbb{N}}$ *be an increasing sequence of positive integers such that* $(a_n - n)_{n\in\mathbb{N}}$ *is unbounded,* $a_0 = 0$, *and let* $(b_n)_{n\in\mathbb{N}}$ *be its complementary sequence. Then*

$$b_n = n + u_n + 1, \tag{4}$$

where

$$u_n = \max\{k \in \mathbb{N} \mid a_k - k \leq n\}.$$

Proof. Let $n \in \mathbb{N}$. There exists $k \in \mathbb{N}$, $k = u_n$ such that

$$a_k - k \leq n < a_{k+1} - (k+1). \tag{5}$$

From proposition 1, $b_n = n + k + 1$ or $b_n = n + u_n + 1$.

Note that the problem of finding the general term of the complementary sequence $(b_n)_{n\in\mathbb{N}}$ is to solve the inequality (5). In other words, we must determine the greatest integer k so that $a_k - k \leq n$ for given n. Let us consider the increasing sequence of nonnegative even integers, $a_n = 2n$, $n \in \mathbb{N}$. The inequality (5) can be written as

$$2k - k \leq n < 2k + 2 - (k+1)$$

or $k \leq n < k + 1$, so $k = n$. Hence $u_n = n$ and consequently,

$$b_n = n + u_n + 1 \Rightarrow b_n = 2n + 1.$$

As we have expected, the complementary sequence of nonnegative even numbers is the sequence of nonnegative odd numbers. We just deduced this result using the previous propositions.

One can easily verify that the complementary sequence of odd numbers is the sequence of nonnegative even numbers. This result is general; if $(b_n)_{n\in\mathbb{N}}$ is the complementary sequence of $(a_n)_{n\in\mathbb{N}}$, then $(a_n)_{n\in\mathbb{N}}$ is the complementary sequence of $(b_n)_{n\in\mathbb{N}}$.

Problem. Find the complementary sequence of the sequence of squares of integers, $a_n = n^2$, $n \in \mathbb{N}$.

Solution. The inequality (5) can be written as

$$k^2 - k \leq n < (k+1)^2 - (k+1) \Leftrightarrow k^2 - k \leq n < k^2 + k$$

$$\Leftrightarrow (2k-1)^2 \leq 4n + 1 < (2k+1)^2 \Leftrightarrow 2k - 1 \leq \sqrt{4n+1} < 2k + 1$$

$$\Leftrightarrow k \leq \frac{1 + \sqrt{4n+1}}{2} < k + 1,$$

thus

$$k = \left[\frac{1 + \sqrt{4n+1}}{2}\right].$$

Now, using (4), we deduce that

$$b_n = n + \left[\frac{1+\sqrt{4n+1}}{2}\right] + 1$$

or

$$b_n = n + \left[\frac{3+\sqrt{4n+1}}{2}\right], \quad n \in \mathbb{N}.$$

The following problem was proposed for the IMO 1978. Even from the statement, one realizes that it concerns complementary sequences.

Problem. The set of positive integers is the disjoint union of two sequences $f(1) < f(2) < \ldots$ and $g(1) < g(2) < \ldots$. Moreover,

$$g(n) = f(f(n)) + 1 \text{ for all } n.$$

Find $f(240)$.

Solution. Because $f(f(n))$ belongs to the first sequence, there are exactly $n-1$ terms of the second sequence smaller than $f(f(n))$, thus

$$f(f(n)) = f(n) + n - 1.$$

Now, clearly 1 is not a member of the second sequence, so $f(1) = 1$ and so the first term of the second sequence is $1 + f(f(1)) = 2$. Because the second sequence does not contain two consecutive numbers, it follows that $f(2) = 3$. But then

$$f(3) = f(f(2)) = f(2) + 2 - 1 = 4,$$

$$f(4) = f(3) + 3 - 1 = 6, \ f(6) = f(4) + 4 - 1 = 9,$$

and also, using the same technique,

$$f(9) = 14, \ f(14) = 22, \ f(22) = 35, \ f(35) = 56, \ f(56) = 90, \ f(90) = 145,$$

and finally,

$$f(145) = 234, \ f(234) = 378.$$

Now, observe that $91 = f(f(35)) + 1$ belongs to the second sequence, so 92 belongs to the first one and $f(57) = 92$. Therefore

$$f(92) = 148 \text{ and } f(148) = 239.$$

Finally, $f(239) = 386$ and so $387 = 1 + f(f(148))$ is a term of the second sequence, which implies that $f(240) = 388$.

The following example is a famous result due to Beatty.

Problem. For positive real numbers a, b, the following two assertions are equivalent:

a) The sequences $([na])_{n\geq 1}$ and $([nb])_{n\geq 1}$ are complementary;

b) a and b are irrational numbers with $\dfrac{1}{a}+\dfrac{1}{b}=1$.

Solution. One implication uses a little bit of analysis: let us assume a). Then for all N, the number of terms of the sequence $[na]$ which do not exceed N plus the number of terms of the sequence $[bn]$ which do not exceed N is exactly N. Note however that if k_N is defined by

$$[k_N a] \leq N < [(k_N+1)a],$$

then there are k_N terms of the sequence $[na]$ not exceeding N. Define r_N similarly for the sequence $[bN]$ and observe that we have $k_N + r_N = N$. However, the above inequalities imply

$$k_N + r_N \leq (N+1)\left(\frac{1}{a}+\frac{1}{b}\right)$$

and also

$$k_N + r_N > N\left(\frac{1}{a}+\frac{1}{b}\right) - 2.$$

By dividing these inequalities by N and passing to the limit, we deduce that

$$\frac{1}{a}+\frac{1}{b}=1.$$

Now, this relation shows that in order to prove b), it is sufficient to prove that at least one of the numbers a, b is irrational.
Assuming the contrary, we easily see that the two sequences have common terms: if $a=\dfrac{p}{q}$, $b=\dfrac{p'}{q'}$, then $[qp'a]=[pq'b]$, contradicting the fact that the two sequences are complementary. Therefore a, b are irrational numbers, and the first implication is proved.
Assume now that b) holds. Let us find the greatest k such that $[ka]-k\leq n$. We have, by definition of k, the inequalities $[ka]\leq n+k$, from where $k<\dfrac{n+1}{a-1}$ and $[ka+a]\geq n+k+2$, which implies $k\geq\dfrac{n+1}{a-1}-1$. Therefore, by taking into account the fact that a is not rational, we can write $k=\left[\dfrac{n+1}{a-1}\right]$. But then $k+n+1=[(n+1)b]$, because $b=\dfrac{a}{a-1}$. By taking into account the "shift" of indices and the theoretical part discussed in the beginning of the chapter, we can assert that $([bn])$ is the complementary sequence of $([an])$. This finishes the proof of the other implication.

Proposed Problems

1. Let us assume that $(b_n)_{n\in\mathbb{N}}$ is the complementary sequence of the sequence $(n+a_n)_{n\in\mathbb{N}}$. Find in terms of $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ the complementary sequence of the sequence $(n+2a_n)_{n\in\mathbb{N}}$.

2. Find the complementary sequence of the sequence $(a_n)_{n\in\mathbb{N}}$ given by the formula
$$a_n = n^3 + 3n^2 + 4n.$$

3. Find the complementary sequence of the sequence $(a_n)_{n\in\mathbb{N}}$ given by
$$a_n = n + \left[\sqrt{n} + \sqrt[4]{n}\right].$$

4. Solve in the set of integers the equation $n + \left[\sqrt{n} + \dfrac{1}{2}\right] = m^2$.

5. Prove that the numbers $n + \left[\dfrac{3+\sqrt{8n+1}}{2}\right]$, $n \in \mathbb{N}$, cannot be triangular numbers. (A *triangular number* is a number of the form $t(t+1)/2$, where t is positive integer.)

6. Prove that the numbers $N = n + \left[\dfrac{n+26}{99}\right]$, $n \in \mathbb{N}$, cannot have the last two digits 73. In other words, the congruence $N \equiv 73 (\mathrm{mod}\ 100)$ is impossible.

7. Solve in the set of integers the equation $n + [\log_2 n] + 2 = m + 2^{m-1}$.

8. Find the complementary sequence of the sequence $a_n = n + [\sqrt{n}]$, $n \in \mathbb{N}$.

9. Find the sum $\sigma = \sum\limits_{n=1}^{10000} [\sqrt{n}]$.

10. Let $(b_n)_{n\in\mathbb{N}}$ be the complementary sequence of the sequence $(a_n)_{n\in\mathbb{N}}$. Prove that if $a_k - b_p = 1$ for some nonnegative integers k and p, then $a_k = k+p+1$ and $b_p = k+p$.

11. Let $\phi = (1+\sqrt{5})/2$ be the golden ratio, and let $a_n = [n\phi]$ and $b_n = [n\phi^2]$, for positive integers n. Let $(f_n)_{n\geq 0}$ be the Fibonacci sequence, defined by $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$. Prove the following properties of the complementary sequences $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$:

    (a) $a_n + b_n = a_{b_n} = b_{a_n} + 1$ for all $n \geq 1$.

    (b) $a_{f_n} = f_{n+1} - 1$ and $b_{f_n} = f_{n+2} - 1$ for even n, while $a_{f_n} = f_{n+1}$ and $b_{f_n} = f_{n+2}$ for odd n.

12. Show that the equation

$$\left[\frac{n+1}{\phi}\right] = n - \left[\frac{n}{\phi}\right] + \left[\frac{[n/\phi]}{\phi}\right] - \left[\frac{\left[\frac{[n/\phi]}{\phi}\right]}{\phi}\right] + \cdots$$

holds for every nonnegative integer n if and only if $\phi = (1+\sqrt{5})/2$.

Solutions

1. The complementary sequence of the sequence $(n+2a_n)_{n\in\mathbb{N}}$ is $\left(b_{[n/2]}\right)_{n\in\mathbb{N}}$. According to the theoretical results, we have $b_n = n+u_n+1$, where $u_n = \max\{k \mid a_k \le n\}$. If $(b'_n)_{n\in\mathbb{N}}$ is the complementary sequence of the sequence $(n+2a_n)_{n\in\mathbb{N}}$, then $b'_n = n + v_n + 1$, where $v_n = \max\{k \mid 2a_k \le n\}$. We have

$$2a_k \le n \Leftrightarrow a_k \le \frac{n}{2} \Leftrightarrow a_k \le \left[\frac{n}{2}\right].$$

From the definition of u_n, the greatest integer with the property that $a_k \le \left[\frac{n}{2}\right]$ is equal to $u_{[n/2]}$, so $v_n = u_{[n/2]}$. In conclusion,

$$b'_n = n + u_{[n/2]} + 1 = b_{[n/2]}.$$

2. The complementary sequence $(b_n)_{n\in\mathbb{N}}$ is given by

$$b_n = n + [\sqrt[3]{n+1}].$$

Thus, let us determine $u_n = \max\{k \mid a_k - k \le n\}$. We have

$$a_k - k \le n \Leftrightarrow k^3 + 3k^2 + 3k \le n$$

and by adding 1,

$$(k+1)^3 \le n+1 \Leftrightarrow k+1 \le \sqrt[3]{n+1}.$$

This is equivalent to $k+1 \le [\sqrt[3]{n+1}]$, so the greatest number k with this property is

$$u_n = [\sqrt[3]{n+1}] - 1.$$

Consequently,

$$b_n = n + u_n + 1 = n + [\sqrt[3]{n+1}].$$

3. The complementary sequence of the sequence $(a_n)_{n\in\mathbb{N}}$ is

$$b_n = n + \left[\left(\sqrt{n+\frac{5}{4}}-\frac{1}{2}\right)^4\right] + 1.$$

We need to find $u_n = \max\{k \mid a_k - k \leq n\}$.

We have

$$a_k - k \leq n \Leftrightarrow \left[\sqrt{k}+\sqrt[4]{k}\right] \leq n.$$

This is equivalent to $\sqrt{k}+\sqrt[4]{k} < n+1$. By adding 1/4, we obtain

$$\left(\sqrt[4]{k}+\frac{1}{2}\right)^2 < n+\frac{5}{4}$$

so

$$\sqrt[4]{k}+\frac{1}{2} < \sqrt{n+\frac{5}{4}} \Leftrightarrow k < \left(\sqrt{n+\frac{5}{4}}-\frac{1}{2}\right)^4.$$

Thus the greatest integer k which satisfies the previous relation is

$$u_n = \left[\left(\sqrt{n+\frac{5}{4}}-\frac{1}{2}\right)^4\right].$$

Consequently,

$$b_n = n + \left[\left(\sqrt{n+\frac{5}{4}}-\frac{1}{2}\right)^4\right] + 1.$$

4. $b_n = n + \left[\dfrac{3+\sqrt{4n+1}}{2}\right]$, $n \in \mathbb{N}$ is the complementary sequence of the sequence of squares. We will prove that

$$\left[\frac{1+\sqrt{4n+1}}{2}\right] = \left[\sqrt{n+1}+\frac{1}{2}\right], \tag{1}$$

so the given equation can be written as

$$n + \left[\sqrt{n}+\frac{1}{2}\right] = m^2 \Leftrightarrow b_{n-1} = m^2,$$

for $n \geq 1$. Obviously, $n = 0$ is the unique solution of the given equation. In order to prove (1), we assume that

$$\frac{1+\sqrt{4n+1}}{2} < k < \sqrt{n+1}+\frac{1}{2},$$

for some positive integer k. Then

$$\frac{1+\sqrt{4n+1}}{2} < k \Rightarrow \sqrt{4n+1} < 2k-1$$
$$\Rightarrow n < k^2-k \Rightarrow n \le k^2-k-1.$$

On the other hand,

$$k < \sqrt{n+1}+\frac{1}{2} \Rightarrow \sqrt{n+1} > k-\frac{1}{2}$$
$$\Rightarrow n+1 > k^2-k+\frac{1}{4} \Rightarrow n > k^2-k-\frac{3}{4},$$

which is a contradiction.

5. We prove that $b_n = n + \left[\frac{3+\sqrt{8n+1}}{2}\right]$ is the complementary sequence of the sequence of triangular numbers. In this sense, from

$$a_k - k \le n < a_{k+1}-(k+1),$$

with $a_k = \frac{k(k+1)}{2}$, we deduce that

$$\frac{k(k+1)}{2} - k \le n < \frac{(k+1)(k+2)}{2} - (k+1)$$
$$\Rightarrow k^2-k \le 2n < k^2+k \Rightarrow 4k^2-4k+1 \le 8n+1 < 4k^2+4k+1$$
$$\Rightarrow 2k-1 \le \sqrt{8n+1} < 2k+1 \Rightarrow k \le \frac{1+\sqrt{8n+1}}{2} < k+1,$$

so $k = \left[\frac{1+\sqrt{8n+1}}{2}\right]$. In conclusion,

$$b_n = n+k+1 = n+\left[\frac{3+\sqrt{8n+1}}{2}\right].$$

6. $b_n = n+\left[\frac{n+26}{99}\right]$, $n \in \mathbb{N}$ is the complementary sequence of the sequence $a_n = 100n+73$. Indeed,

$$a_k - k \le n < a_{k+1}-(k+1) \Rightarrow 99k+73 \le n < 99k+172$$
$$\Rightarrow k \le \frac{n-73}{99} < k+1,$$

so $k = \left[\frac{n-73}{99}\right]$. Finally,

$$b_n = n+k+1 = n+\left[\frac{n+26}{99}\right].$$

7. Let us find the complementary sequence of the sequence $a_n = n + 2^{n-1}$. We have

$$a_k - k \le n < a_{k+1} - (k+1) \Rightarrow 2^{k-1} \le n < 2^k,$$

so $k = [\log_2 n] + 1$. Then

$$b_n = n + k + 1 = n + [\log_2 n] + 2.$$

8. With $a_n = n + [\sqrt{n}]$, we have

$$a_k - k \le n < a_{k+1} - (k+1) \Rightarrow \left[\sqrt{k}\right] \le n < \left[\sqrt{k+1}\right],$$

so $k = n^2 + 2n$. Finally, $b_n = n + k + 1 = n^2 + 3n + 1$.

9. As we have proved, $b_n = n + [\sqrt{n}]$ is the complementary sequence of the sequence $a_n = n^2 + 3n + 1$. Let us consider the sum

$$S = \sum_{n=1}^{10000} (n + [\sqrt{n}])$$

or

$$S = b_1 + b_2 + \ldots + b_{10000}.$$

Then

$$S = \sum_{n=1}^{10000} (n + [\sqrt{n}]) = 50{,}005{,}000 + \sum_{n=1}^{10000} [\sqrt{n}].$$

so

$$S = 50{,}005{,}000 + \sigma.$$

Because $10100 = b_{10000}$ and $10099 = a_{99}$, we have

$$(a_1 + a_2 + \ldots + a_{99}) + (b_1 + b_2 + \ldots + b_{10000}) = 1 + 2 + 3 + \ldots + 10100,$$

or

$$(a_1 + a_2 + \ldots + a_{99}) + S = 51{,}010{,}050.$$

Hence

$$S = 51{,}010{,}050 - \sum_{n=1}^{99} a_n$$

$$= 51{,}010{,}050 - \sum_{n=1}^{99}(n^2 + 3n + 1) - 50{,}005{,}000 = 661{,}750.$$

We can give also a direct proof, without using the theory of complementary sequences. In order to express the integral part, we write for positive integers k,

$$[\sqrt{n}] = k \Leftrightarrow k \le \sqrt{n} < k+1 \Leftrightarrow k^2 \le n < (k+1)^2$$

or

$$[\sqrt{n}] = k \Leftrightarrow n \in \{k^2, k^2+1, k^2+2, \ldots, k^2+2k\}.$$

Hence

$$\begin{aligned}\sigma = \sum_{n=1}^{10000} [\sqrt{n}] = &\left([\sqrt{1}] + [\sqrt{2}] + [\sqrt{3}]\right) + \\ &+ \left([\sqrt{4}] + [\sqrt{5}] + [\sqrt{6}] + [\sqrt{7}] + [\sqrt{8}]\right) + \ldots \\ &+ \left([\sqrt{k^2}] + [\sqrt{k^2+1}] + \ldots + [\sqrt{k^2+2k}]\right) + \ldots \\ &+ \left([\sqrt{99^2}] + [\sqrt{99^2+1}] + \ldots + [\sqrt{99^2+2\cdot 99}]\right) + \\ &+ [\sqrt{10000}]\end{aligned}$$

Taking into account that all terms lying on the same line are equal and by using the sum symbol, we deduce that

$$\sigma = \sum_{k=1}^{99} \left(\sum_{p=0}^{2k} [\sqrt{k^2+p}] \right) + [\sqrt{10000}]$$

or successively

$$\begin{aligned}\sigma &= 100 + \sum_{k=1}^{99} \left(\sum_{p=0}^{2k} k \right) = 100 + \sum_{k=1}^{99} k(2k+1) \\ &= 100 + \sum_{k=1}^{99} (2k^2 + k) = 100 + 2\sum_{k=1}^{99} k^2 + \sum_{k=1}^{99} k.\end{aligned}$$

Now, with the formulas

$$\sum_{k=1}^{w} k = \frac{w(w+1)}{2}, \quad \sum_{k=1}^{w} k^2 = \frac{w(w+1)(2w+1)}{6},$$

we have in particular,

$$\sum_{k=1}^{99} k^2 = 328{,}350, \quad \sum_{k=1}^{99} k = 4950.$$

Thus

$$\sigma = 100 + 2 \cdot 328{,}350 + 4950 = 661{,}750.$$

10. Let us define the sets

$$A = \{a_0, a_1, \ldots, a_k\}, \quad B = \{b_0, b_1, \ldots, b_p\}.$$

According to the definition of the complementary sequences, the sets A and B are disjoint. Because

$$0 \leq a_0 < a_1 < \ldots < a_k$$

and

$$0 \leq b_0 < b_1 < \ldots < b_p = a_k - 1,$$

it follows that

$$A \cup B \subseteq \{0, 1, 2, \ldots, a_k\}.$$

The reverse inclusion is also true. Indeed, if $q \in \{0, 1, 2, \ldots, a_k - 1\}$, then there exists a_i or b_j such that

$$q = a_i \quad \text{or} \quad q = b_j.$$

The sequences $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are increasing, so from

$$a_i = q \leq a_k \quad \text{or} \quad b_j = q \leq a_k - 1 = b_p,$$

it follows that $i \leq k$, respectively $j \leq p$. In any case, $q \in A \cup B$, so

$$A \cup B = \{0, 1, 2, \ldots, a_k\}.$$

Thus

$$(a_0 + a_1 + \ldots + a_k) + (b_0 + b_1 + \ldots + b_p) = 0 + 1 + 2 + \ldots + a_k.$$

There are $k + p + 2$ terms in the left hand of the previous equality, so we have the first $k + p + 2$ nonnegative integers. It follows that

$$(a_0 + a_1 + \ldots + a_k) + (b_0 + b_1 + \ldots + b_p) = 0 + 1 + 2 + \ldots + (k + p + 1).$$

By comparing with the above relation, it follows that $a_k = k + p + 1$ and consequently, $b_p = k + p$.

11. Indeed, $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$ are complementary sequences, by Beatty's theorem (because ϕ and ϕ^2 are irrational numbers and $1/\phi + 1/\phi^2 = 1$, as ϕ satisfies the quadratic equation $\phi^2 = \phi + 1$).

(a) We have to prove that $[n\phi] + [n\phi^2] = \left[[n\phi^2]\phi\right] = \left[[n\phi]\phi^2\right] + 1$ for every positive integer n. First note that we have $[n\phi^2] < n\phi^2 < [n\phi^2] + 1$ (the first inequality from the definition of the greatest integer function could be an equality, but not in the case of an irrational number, like $n\phi^2$), thus

$$n - \frac{1}{\phi^2} < \frac{[n\phi^2]}{\phi^2} < n$$

and, since $0 < 1/\phi^2 < 1$, we get

$$\left[\frac{[n\phi^2]}{\phi^2}\right] = n - 1.$$

Also, we have $1/\phi^2 = 1 - 1/\phi$, hence the above relation becomes

$$\left[[n\phi^2] - \frac{[n\phi^2]}{\phi}\right] = n - 1 \Leftrightarrow [n\phi^2] - \left[\frac{[n\phi^2]}{\phi^2}\right] - 1 = n - 1$$

(we used $[x+p] = [x]+p$ for real x and integer p, and $[-x] = -[x]-1$ when x is not an integer). But here we can replace $[n\phi^2] = [n\phi+n] = [n\phi]+n$, and thus obtain

$$\left[\frac{[n\phi^2]}{\phi^2}\right] = [n\phi].$$

Finally, because $\phi = 1 + 1/\phi$, we have $[n\phi] = n + [n/\phi]$, therefore (by replacing here n with $[n\phi^2]$)

$$[[n\phi^2]\phi]] = [n\phi^2] + \left[\frac{[n\phi^2]}{\phi}\right] = [n\phi^2] + [n\phi],$$

as required.

For the second equality, observe that we can prove

$$\left[\frac{[n\phi]}{\phi}\right] = n - 1,$$

in the exact same way as we proved above the formula $\left[[n\phi^2]/\phi^2\right] = n-1$. Replacing here $1/\phi = \phi - 1$ yields $[[n\phi]\phi] = [n\phi] + n - 1$, hence

$$[[n\phi]\phi^2] = [[n\phi]\phi + [n\phi]] = [[n\phi]\phi] + [n\phi] = 2[n\phi] + n - 1.$$

On the other hand, as we already proved,

$$[[n\phi^2]\phi] = [n\phi^2] + [n\phi] = [n\phi + n] + [n\phi] = 2[n\phi] + n = [[n\phi]\phi^2] + 1,$$

and the first part is solved.

(b) We have

$$f_n = \frac{1}{\sqrt{5}}\left(\phi^n - \left(-\frac{1}{\phi}\right)^n\right),$$

thus, for example,

$$\begin{aligned}a_{f_{2m}} = [f_{2m}\phi] &= \left[\frac{1}{\sqrt{5}}\left(\phi^{2m} - \frac{1}{\phi^{2m}}\right)\phi\right] = \left[\frac{1}{\sqrt{5}}\left(\phi^{2m+1} - \frac{1}{\phi^{2m-1}}\right)\right] \\ &= \left[\frac{1}{\sqrt{5}}\left(\phi^{2m+1} + \frac{1}{\phi^{2m+1}}\right) - \frac{1}{\sqrt{5}}\left(\frac{1}{\phi^{2m+1}} + \frac{1}{\phi^{2m-1}}\right)\right] \\ &= f_{2m+1} + \left[-\frac{1}{\sqrt{5}}\left(\frac{1}{\phi^{2m+1}} + \frac{1}{\phi^{2m-1}}\right)\right] = f_{2m+1} - 1.\end{aligned}$$

The last integer part is -1 because the expression inside it can be evaluated:

$$-\frac{1}{\sqrt{5}}\left(\frac{1}{\phi^{2m+1}} + \frac{1}{\phi^{2m-1}}\right) = -\frac{1+\phi^2}{\phi^{2m+1}\sqrt{5}} = -\frac{1}{\phi^{2m}}$$

(since $1+\phi^2 = 2+\phi = \phi\sqrt{5}$), and $0 < 1/\phi^{2m} < 1$.

The reader will surely be able to solve similarly all the other cases. The formula $b_n = a_n + n$ can also be used for calculating b_n with the help of a_n (or vice versa) when the index n is a term of the Fibonacci sequence.

Part (a) is problem 11238 proposed by Aviezri S. Fraenkel in *The American Mathematical Monthly*, 7/2006, and solved by Reiner Martin in the same magazine, number 7/2008. Part (b) is a problem from a Romanian TST, back in the year 1982.

12. Let $\alpha = (\sqrt{5}-1)/2$. We first prove that

$$[(n+1)\alpha] + [([n\alpha]+1)\alpha] = n$$

for every nonnegative integer n. Note that $\alpha^2 = 1-\alpha$ and let $p = [n\alpha]$; we have two possibilities.

First, when $p < n\alpha < (n+1)\alpha < p+1$, we have $[(n+1)\alpha] = p$ as well, hence we need to prove

$$\begin{aligned}[(p+1)\alpha] = n-p &\Leftrightarrow n-p < (p+1)\alpha < n-p+1 \\ &\Leftrightarrow (n-p)\alpha < (p+1) - (p+1)\alpha < (n-p+1)\alpha \\ &\Leftrightarrow (n+1)\alpha < p+1 < (n+2)\alpha.\end{aligned}$$

Here the left inequality is true as assumed, and the right inequality is true because if it wasn't, we would have $p < n\alpha < (n+2)\alpha \le p+1$, which would imply $1 = (p+1) - p > (n+2)\alpha - n\alpha = 2\alpha = \sqrt{5}-1$, which is false.

The second case is $p < n\alpha < p+1 < (n+1)\alpha < p+2$, and now we have to show that

$$[(p+1)\alpha] = n-p-1 \Leftrightarrow n-p-1 < (p+1)\alpha < n-p$$

$$\Leftrightarrow (n-p-1)\alpha < (p+1)-(p+1)\alpha < (n-p)\alpha$$

$$\Leftrightarrow n\alpha < p+1 < (n+1)\alpha,$$

which is clear.

Now, for the problem, assume first that $\phi = (1+\sqrt{5})/2$, that is, $\phi = 1/\alpha$. The equality that we proved is, in terms of ϕ:

$$\left[\frac{n+1}{\phi}\right] = n - \left[\frac{\left[\frac{n}{\phi}\right]+1}{\phi}\right].$$

All that one has to do in order to get the equation required by the problem statement is to evaluate the second term from the right hand side using the same equality with $[n/\phi]$ in place of n; then do the same with the last term (with n replaced by $[n/\phi]$ in the equation where we already have made this replacement once), and so on.

Conversely, suppose that the equation given in the problem statement holds for any nonnegative integer n. For $n = 0$, we see that $\phi > 0$ is necessary. By comparing with the same equation where n is replaced by $[n/\phi]$, we get that

$$\left[\frac{n+1}{\phi}\right] = n - \left[\frac{\left[\frac{n}{\phi}\right]+1}{\phi}\right]$$

also holds for all nonnegative integers n. If we divide this equation by n and pass to the limit for $n \to \infty$, we obtain

$$\frac{1}{\phi} = 1 - \frac{1}{\phi^2} \Leftrightarrow \phi^2 - \phi - 1 = 0,$$

therefore $\phi = (1+\sqrt{5})/2$ follows (since we know that it must be positive), finishing our proof.

This is problem 16551, proposed by Marcel Celaya and Frank Ruskey in *The American Mathematical Monthly*, 6/2012, and solved by O. P. Lossers, in 6/2014.

Remark. Our solution is slightly different from O. P. Lossers' solution, which uses the fact that

$$\left[\frac{\left[\frac{n}{\phi}\right]+1}{\phi}\right] = \left[\frac{n+1}{\phi^2}\right],$$

thus reducing the crucial (for this problem) equality

$$\left[\frac{n+1}{\phi}\right] = n - \left[\frac{\left[\frac{n}{\phi}\right]+1}{\phi}\right] \quad \text{to} \quad \left[\frac{n+1}{\phi}\right] + \left[\frac{n+1}{\phi^2}\right] = n.$$

This can be proved immediately by using $1/\phi^2 = 1 - 1/\phi$, but the interesting fact for us is that it can be obtained also by a simple counting argument. Namely, if we consider again the sequences with general terms $a_n = [n\phi]$ and $b_n = [n\phi^2]$ (from the previous problem), then $[(n+1)/\phi]$ and $[(n+1)/\phi^2]$ represent the number of terms of the complementary sequences $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$ respectively that are not greater than n; of course, the sum of these two numbers is n. The reader is invited to prove the facts mentioned in this remark.

Finally, let us say yet that sequences $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$ are called the *Wythoff sequences*; their first few terms are $1, 3, 4, 6, 8, 9, 11, 12, 14, \ldots$ and $2, 5, 7, 10, 13, 15, 18, 20, 23, \ldots$, respectively.

Chapter 7

Quadratic Functions and Quadratic Equations

A quadratic function defined on the reals is a map $f : \mathbb{R} \to \mathbb{R}$ of the form

$$f(x) = ax^2 + bx + c$$

for $a, b, c \in \mathbb{R}$ and $a \neq 0$. The graph of this function is called a parabola. Observe that

$$f(x) - f(y) = a(x-y)\left(x + y + \frac{b}{a}\right),$$

thus

$$f(x) = f(y) \Leftrightarrow x = y \quad \text{or} \quad x + y = -\frac{b}{a}.$$

Therefore, $x = -\frac{b}{2a}$ is a symmetry axis of the parabola associated to f. The previous formula also shows that if $a > 0$, then f is decreasing on $\left(-\infty, -\frac{b}{2a}\right]$ and increasing on $\left[-\frac{b}{2a}, \infty\right)$. If x_1, x_2 are the roots of the equation $f(x) = 0$, then $x_1 + x_2 = -\dfrac{b}{a}$ and $x_1x_2 = \dfrac{c}{a}$, which are called Viète's formulas. Observe that they follow from the fact that $f(x) = a(x - x_1)(x - x_2)$. This last formula also shows that if $a > 0$ and x_1 and x_2 are real, then f is negative between the roots and positive outside the interval determined by its roots.

Even though all of these results may seem very elementary, they do have surprising applications. We present some of them, with different ideas, but all boiling down to quadratic equations or functions. The first problem appeared in the Romanian National Mathematical Olympiad in 1994:

Problem. Let a, b, c, A, B, C be positive real numbers such that the equations $ax^2 - bx + c = 0$ and $Ax^2 - Bx + C = 0$ have real solutions. Prove that for any u between the roots of the first equation and for any U between the roots of the second equation, we have the inequality

$$(au + AU)\left(\frac{c}{u} + \frac{C}{U}\right) \le \left(\frac{b+B}{2}\right)^2.$$

Solution. Of course, from Viète's relations it follows that both equations have positive real roots. Let

$$f(x) = ax^2 - bx + c \quad \text{and} \quad F(x) = Ax^2 - Bx + C.$$

By the previous observations and the hypothesis of the problem, we know that $f(u) \le 0$ and $F(U) \le 0$. This can be also written in the form $au + \frac{c}{u} \le b$ and $AU + \frac{C}{U} \le B$. Therefore

$$b + B \ge (au + AU) + \left(\frac{c}{u} + \frac{C}{U}\right).$$

By combining the last inequality and the AM-GM inequality, we obtain immediately the desired estimation.

The next problem is an adaptation of a Vietnamese problem. It is not immediate, but the argument should be known, since it appears in many problems of this type.

Problem. Prove that there exist integers a, b, c, d greater than 2007 such that

$$a^2 + b^2 + c^2 + d^2 = abcd + 6.$$

Solution. Let us find a solution with small values of a, b, c, d and then see how to produce larger solutions. One can easily check that $(a, b, c, d) = (1, 2, 2, 3)$ is a solution of the equation. The idea is to consider this equation as a quadratic equation in a (or b, c, d) and to use Viète's relations in order to obtain new solutions. Indeed, considering the given relation as a quadratic equation in a, we find that if (a, b, c, d) is a solution, then so is $(bcd - a, b, c, d)$ and also any permutation of the variables, since the equation is symmetric. Thus $(2, 2, 3, 11)$ is also a solution of the equation and applying the argument again, we find the solution $(2, 3, 11, 64)$. Now, if $2 \le a < b < c < d$ are components of a solution, then $b < c < d < bcd - a$ is another solution. The last inequality follows easily because $bcd - d = d(bc - 1) \ge 3d > a$. Thus we can always create a solution whose smallest component is greater than the smallest component of a previous solution. In particular, we can find a solution whose smallest component is greater than 2007.

Problem. Let P be a polynomial with real coefficients such that $P(x) > 0$ for all $x > 0$. Prove that there exist polynomials Q, R with nonnegative coefficients such that

$$P(X) = \frac{Q(X)}{R(X)}.$$

Solution. Here, the essential argument is that every polynomial with real coefficients can be factored as a product of linear and quadratic polynomials with real coefficients. Call a polynomial *good* if it can be written as $P(X) = \frac{Q(X)}{R(X)}$, where P, Q have nonnegative coefficients. It is clear that the product of two good polynomials is good. Thus, it is enough to prove that P is a product of good polynomials. Because $P(x) > 0$ for all $x > 0$, so any linear factor of P must be of the form $X + a$ with $a > 0$, thus any linear factor of P is good. Consider now a quadratic factor of P, which has no real zeros. It can be written as $X^2 - 2aX + b^2$, with $a^2 < b^2$. If $a < 0$, this factor is good, so assume that $a > 0$. We will prove that it is still a good polynomial. The following identity proves to be very useful:

$$(X^2 + b^2)^{2n} - (2aX)^{2n} = (X^2 - 2aX + b^2) \sum_{k=0}^{2n-1} (X^2 + b^2)^k (2aX)^{2n-k-1}.$$

It shows that the problem reduces to proving the existence of a number n such that

$$\binom{2n}{n} > 4^n \left(\frac{a^2}{b^2}\right)^n.$$

Because $\binom{2n}{n}$ is the largest among the binomial coefficients $\binom{2n}{k}$, and because $\sum_{k=0}^{2n} \binom{2n}{k} = 4^n$ it follows that $\binom{2n}{n} \geq \frac{4^n}{2n+1}$. Thus it is enough to prove the existence of n such that $\left(\frac{b^2}{a^2}\right)^n > 2n + 1$, which is clear because

$$\lim_{n\to\infty} \frac{\left(\frac{b^2}{a^2}\right)^n}{2n+1} = \infty.$$

This shows that all factors of P are good, so P is also good.

The use of quadratic equations is not clear from the statement of the following problem.

Problem. Find all positive rational numbers x, y, z such that

$$x + \frac{1}{y}, \quad y + \frac{1}{z}, \quad z + \frac{1}{x}$$

are all integers.

Solution. Let us put $a = x + \frac{1}{y}$, $b = y + \frac{1}{z}$, $c = z + \frac{1}{x}$. Then

$$y = \frac{1}{a - x}, \quad z = \frac{1}{b - y} = \frac{a - x}{ab - 1 - bx},$$

hence,

$$\frac{a-x}{ab-1-bx}+\frac{1}{x}=c \Rightarrow (bc-1)x^2+(a-b+c-abc)x+ab-1=0.$$

Clearly, if $bc=1$ then $b=c=1$ and so $a=1$, which is impossible. The discriminant of the quadratic equation is

$$\Delta=(abc-a-b-c)^2-4.$$

Because $x \in \mathbb{Q}$, Δ is a square. This cannot happen unless $|abc-a-b-c|=2$. Now, because

$$abc-a-b-c=a(bc-1)-b-c \geq bc-1-b-c \geq -2,$$

the relation $abc-a-b-c=-2$ implies $bc=1$, a contradiction.

Similarly, we cannot have $abc=a+b+c+2$ unless one of a, b, c is 1 or 2. If $a=1$, we obtain $(b-1)(c-1)=4$, thus $(b,c)=(3,3)$ or (2,5). If $a=2$, then $(2b-1)(2c-1)=9$, thus (b,c) is (2,2) or (1,5) or (5,1). Finally, the triples are

$$(x,y,z)=\left(\frac{1}{3},\frac{3}{2},2\right), \left(\frac{1}{2},2,1\right), \left(\frac{2}{3}, 3, \frac{1}{2}\right), (1,1,1)$$

and similarly for $a=2$, $b=1$, $c=5$ and permutations.

Proposed Problems

1. Let k be a nonzero integer, and define $\lambda=k+\sqrt{k^2-1}$. Prove that for every integer n, $\lambda^n+\frac{1}{\lambda^n}$ is an even integer.

2. We say that the equations $x^2+ax+b=0$ and $x^2+cx+d=0$ are *friends* if they have real and separated roots. More precisely, if we denote by $x_1<x_2$ and $x_3<x_4$ the roots of the first, respectively of the second equation, then

$$x_1<x_3<x_2<x_4 \quad \text{or} \quad x_3<x_1<x_4<x_2.$$

Prove that the equation

$$x^2+\left(\frac{a+c}{2}\right)x+\left(\frac{b+d}{2}\right)=0$$

has real roots and it is friends with each of the first two equations.

3. For real numbers α, β denote

$$\mathcal{M}(\alpha, \beta) = \{x \in \mathbb{R} \mid x^2 + \alpha x + \beta = 0\}.$$

Let a, b, c be integers. Prove that if

$$\mathcal{M}(a, b) \cup \mathcal{M}(b, c) \cup \mathcal{M}(c, a) = \emptyset,$$

then $a = b = c$.

4. For real numbers α, β, γ denote

$$\mathcal{M}(\alpha, \beta, \gamma) = \{x \in \mathbb{R} \mid \alpha x^2 + \beta x + \gamma = 0\}.$$

Let a, b, c be nonzero real numbers. Prove that if

$$\mathcal{M}(a, b, c) \cap \mathcal{M}(b, c, a) \cap \mathcal{M}(c, a, b) \neq \emptyset,$$

then the set

$$\mathcal{M}(a, b, c) \cup \mathcal{M}(b, c, a) \cup \mathcal{M}(c, a, b)$$

has three or four elements.

5. Let a, b, c be nonzero real numbers such that

$$33(a^6 + b^6 + c^6) \leq 31(a^3 + b^3 + c^3)^2.$$

Prove that we can find a cyclic permutation α, β, γ of a, b, c such that

$$\{x \in \mathbb{R} \mid \alpha x^2 + \beta x + \gamma = 0\} = \emptyset.$$

6. Let a, b, m, n be real numbers such that

$$m^2 + n^2 - a(m + n) + 2b = 0.$$

Prove that $(m + n + a)^2 \geq 8(mn + b)$.

7. Let n be a positive integer. Denote by $\mathcal{F}_n$ the set of all quadratic functions $f : \mathbb{R} \to \mathbb{R}$ satisfying the relation

$$f(f(1)) = f(f(2)) = \ldots = f(f(n)).$$

a) Prove that $\mathcal{F}_n = \emptyset$ for all $n \geq 5$.

b) Determine $\mathcal{F}_4$.

8. Let a, b, c, d be real numbers such that $ad > 0$ and let x_0 be a real root of the third degree equation

$$ax^3 + bx^2 + cx + d = 0.$$

Prove that $x_0 \leq \dfrac{c^2 - 4bd}{4ad}$.

9. Let a, b, c be real numbers, $a \neq 0$. Prove that if a and $4a + 3b + 2c$ have the same sign, then the quadratic equation $ax^2 + bx + c = 0$ cannot have both roots in the interval $(1, 2)$.

10. Let a, b, c be real numbers and let $f : \mathbb{R} \to \mathbb{R}$ be a quadratic function with integer coefficients such that

$$|f(k)| < ak^2 + bk + c + 1,$$

for all integers k. Prove that $b^2 - 4ac < 9a^2$.

11. Let a, b, c, d be real numbers and $f : \mathbb{R} \to \mathbb{R}$ be the function given by

$$f(x) = ax^3 + bx^2 + cx + d.$$

Prove that if

$$f(2) + f(5) < 7 < f(3) + f(4),$$

then there exist two real numbers u and v such that

$$u + v = 7 \quad \text{and} \quad f(u) + f(v) = 7.$$

12. Let $g, h : \mathbb{R} \to \mathbb{R}$ be two quadratic functions and let $f : \mathbb{R} \to \mathbb{R}$ be such that $f \circ g = h$. Prove that there exist two real numbers m, n and an unbounded interval I such that $f(y) = my + n$, for all $y \in I$.

13. Let us denote by $\mathcal{Q}$ the set of all quadratic functions. Prove that if a function $f : \mathbb{R} \to \mathbb{R}$ satisfies the implication:

$$g \in \mathcal{Q} \Rightarrow f \circ g \in \mathcal{Q},$$

then $f(x) = mx + n$, for some real numbers m, n.

14. Let $f, g : \mathbb{R} \to \mathbb{R}$ be two quadratic functions such that if $g(x)$ is an integer, then $f(x)$ is an integer as well. Prove that there exist two integers m and n such that $f(x) = mg(x) + n$, for all real numbers x.

15. Find all functions $f : [0, \infty) \to [0, \infty)$ which satisfy the relation

$$f(x^2 + x) \leq x \leq f^2(x) + f(x),$$

for all nonnegative real numbers x.

16. Let f be a quadratic function such that

$$0 \leq f(-1) \leq 1, \quad 0 \leq f(0) \leq 1, \quad 0 \leq f(1) \leq 1.$$

Prove that $f(x) \leq \frac{9}{8}$, for all real numbers $x \in [-1, 1]$.

17. Let $x \in [0,1]$, $y \in [1,2]$, $z \in [2,3]$ be real numbers. Prove that:

$$\frac{3}{4} \leq x^2 + y^2 + z^2 - xy - yz - zx \leq 7,$$

then find the equality cases.

18. Let a, b, c be positive integers such that $b > a^2 + c^2$. Prove that the roots of the quadratic equation $ax^2 + bx + c = 0$ are irrational.

19. Let a, b, x, y be real numbers, $x, y > 0$, $x \neq y$. Prove that if the equality

$$x^n + y^n = a(x^{n-1} + y^{n-1}) + b(x^{n-2} + y^{n-2})$$

holds for $n = k$ and $n = k + 1$, then it holds for all integers n.

20. Let $a > 2$ be rational. Prove that any integer solution of the equation

$$x^2 - a(a^2 - 3)x + 1 = 0$$

is the cube of an integer.

Solutions

1. Let $x_1 = k + \sqrt{k^2 - 1}$ and $x_2 = k - \sqrt{k^2 - 1} = \dfrac{1}{k + \sqrt{k^2 - 1}}$. Then $x_1 x_2 = 1$ and $x_1 + x_2 = 2k$. We need to show that $x_1^n + x_2^n$ is an even integer for all integers n. First, observe that $x_1^n + x_2^n = x_1^{-n} + x_2^{-n}$, thus it is enough to assume that n is positive. The relations $x_1 x_2 = 1$ and $x_1 + x_2 = 2k$ show that x_1, x_2 are roots of the quadratic equation $x^2 - 2kx + 1 = 0$. Multiplying by x^n gives $x^{n+2} = 2kx^{n+1} - x^n$, thus if $a_n = x_1^n + x_2^n$, we have $a_{n+2} = 2ka_{n+1} - a_n$, which shows that a_n is an even integer for all n (by induction).

2. Denote

$$f(x) = x^2 + ax + b, \quad g(x) = x^2 + cx + d$$

and

$$h(x) = \frac{1}{2}(f(x) + g(x)).$$

If x_1, x_2 and x_3, x_4 are the solutions of the equation $f(x) = 0$, respectively $g(x) = 0$, with $x_1 < x_3 < x_2 < x_4$, then

$$f(x) = x^2 + ax + b = (x - x_1)(x - x_2)$$

$$g(x) = x^2 + cx + d = (x - x_3)(x - x_4).$$

Note that

$$h(x) = \frac{1}{2}\left[(x - x_1)(x - x_2) + (x - x_3)(x - x_4)\right],$$

hence

$$h(x_1) = \frac{1}{2}g(x_1) = \frac{1}{2}(x_1 - x_3)(x_1 - x_4) > 0$$

$$h(x_2) = \frac{1}{2}g(x_2) = \frac{1}{2}(x_2 - x_3)(x_2 - x_4) < 0,$$

and, similarly,

$$h(x_3) = \frac{1}{2}f(x_3) = \frac{1}{2}(x_3 - x_1)(x_3 - x_2) < 0$$

$$h(x_4) = \frac{1}{2}f(x_4) = \frac{1}{2}(x_4 - x_1)(x_4 - x_2) > 0.$$

Because $h(x_1) > 0$, $h(x_2) < 0$, and $h(x_4) > 0$ it follows that h has two distinct real roots $y_1 \in (x_1, x_2)$, and $y_2 \in (x_2, x_4)$; since $x_1 < y_1 < x_2 < y_2$, h and f are friends. Yet, because $h(x_1) > 0$, $h(x_3) < 0$, and $h(x_4) > 0$ we see that $y_1 \in (x_1, x_3)$, and $y_2 \in (x_3, x_4)$, thus $y_1 < x_3 < y_2 < x_4$, that is, h is also friends with g.

3. Clearly,

$$\mathcal{M}(a,b) = \mathcal{M}(b,c) = \mathcal{M}(c,a) = \emptyset,$$

so the equations

$$x^2 + ax + b = 0, \quad x^2 + bx + c = 0, \quad x^2 + cx + a = 0$$

have no real solutions. We impose the conditions

$$a^2 < 4b\,,\; b^2 < 4c\,,\; c^2 < 4a,$$

so $a, b, c \geq 1$. If $a = 1$, then $c^2 < 4 \Rightarrow c = 1$ and similarly, $b = 1$. If $a, b, c \geq 2$, then

$$a > \frac{c^2}{4} > \frac{b^4}{4^3} > \frac{a^8}{4^7} \Rightarrow a^7 < 4^7 \Rightarrow a \leq 3$$

and similarly for b and c. Hence $a, b, c \in \{2, 3\}$. If $a = 3$, then

$$9 < 4b \Rightarrow b > \frac{9}{4} \Rightarrow b = 3$$

and further, $c = 3$. If $a = 2$, then $c^2 < 8$, so $c = 2$ and analogously, $b = 2$.

In conclusion, $a = b = c \in \{1, 2, 3\}$.

4. Suppose

$$\alpha \in \mathcal{M}(a, b, c) \cap \mathcal{M}(b, c, a) \cap \mathcal{M}(c, a, b);$$

then

$$a\alpha^2 + b\alpha + c = 0 \ , \ b\alpha^2 + c\alpha + a = 0 \ , \ c\alpha^2 + a\alpha + b = 0$$

and, by addition,

$$(a + b + c)(\alpha^2 + \alpha + 1) = 0 \Rightarrow a + b + c = 0.$$

Now we see that $1 \in \mathcal{M}(a, b, c) \cap \mathcal{M}(b, c, a) \cap \mathcal{M}(c, a, b)$, and using Viète's relations,

$$\mathcal{M}(a, b, c) = \left\{1, \frac{c}{a}\right\} \ , \ \mathcal{M}(b, c, a) = \left\{1, \frac{a}{b}\right\} \ , \ \mathcal{M}(c, a, b) = \left\{1, \frac{b}{c}\right\}.$$

We cannot have $a = b = c$ (as $a + b + c = 0$ would give $a = b = c = 0$), but it is possible for two of the three numbers to be equal. For instance, the conditions $a = b$ and $a + b + c = 0$ easily yield

$$\mathcal{M}(a, b, c) \cup \mathcal{M}(b, c, a) \cup \mathcal{M}(c, a, b) = \left\{1, -2, -\frac{1}{2}\right\}$$

and the same follows when $a = c$ or $b = c$. Otherwise we surely have

$$\frac{a}{b} \neq 1, \ \frac{b}{c} \neq 1, \ \text{and} \ \frac{c}{a} \neq 1.$$

If we assume, for example, that $\frac{c}{a} = \frac{a}{b}$, then $a^2 = bc$ and

$$(-b - c)^2 = bc \Rightarrow b^2 + bc + c^2 = 0 \Rightarrow \left(b + \frac{c}{2}\right)^2 + \frac{3c^2}{4} = 0,$$

which is possible only for $b = c = 0$ (but this is not allowed). In conclusion, when a, b, and c are mutually distinct

$$\mathcal{M}(a, b, c) \cup \mathcal{M}(b, c, a) \cup \mathcal{M}(c, a, b) = \left\{1, \frac{a}{b}, \frac{b}{c}, \frac{c}{a}\right\}$$

has four elements (and it has three when two of a, b, and c are equal).

5. Assuming the contrary, we obtain

$$a^2 \geq 4bc, \quad b^2 \geq 4ca, \quad c^2 \geq 4ab.$$

Thus

$$a^6+b^6+c^6 \geq 64(a^3b^3+b^3c^3+c^3a^3) = 32[(a^3+b^3+c^3)^2-(a^6+b^6+c^6)]$$

or

$$a^6+b^6+c^6 \geq \frac{32}{33}(a^3+b^3+c^3)^2,$$

which contradicts the hypothesis.

6. Let us define the quadratic equation

$$f(x) = x^2 - ax + b + (x-m)(x-n) = 2x^2 - (m+n+a)x + mn + b.$$

According to the hypotheses,

$$f(m) + f(n) = 0,$$

so the equation $f(x) = 0$ has real solutions (if not, it results in $f(x) > 0$ for all reals x). Consequently,

$$\Delta = (m+n+a)^2 - 8(mn+b) \geq 0.$$

There is another way to prove the inequality that involves a small computation. Namely, replacing $2b$ by $a(m+n) - m^2 - n^2$ and performing the computations, the inequality boils down to

$$5(m^2+n^2) + a^2 \geq 6mn + 2a(m+n),$$

or $3(m^2+n^2) \geq 6mn$ and $2(m^2+n^2)+a^2 \geq (m+n)^2+a^2 \geq 2a(m+n)$. This proves the desired inequality. However, it is very important to have understood this type of argument using quadratic functions, because a very large class of inequalities can be proved using this technique. For instance, prove the Cauchy-Schwarz inequality using quadratic functions.

7. The first question is clear because $f(f(X))$ is a nonzero polynomial of degree 4, so it cannot have more than 4 distinct pre-images. Now, let

$$\alpha = f(f(1)) = f(f(2)) = f(f(3)) = f(f(4))$$

and let y_1, y_2 be the solutions of the quadratic equation $f(y) = \alpha$. Thus

$$f(1), f(2), f(3), f(4) \in \{y_1, y_2\}.$$

If $i \neq j \neq k$, then the equality $f(i) = f(j) = f(k)$ is impossible. Consequently, we must have

$$f(1) = f(4) \quad \text{and} \quad f(2) = f(3).$$

If $f(x) = ax^2 + bx + c$, then $-\dfrac{b}{a} = 1 + 4 = 2 + 3$, so

$$f(x) = ax^2 - 5ax + c,$$

for some $a \neq 0$ and c.
From $f(f(1)) = f(f(2))$ and $f(1) \neq f(2)$, we deduce

$$f(1) + f(2) = -5 \Rightarrow -10a + 2c = -5 \Rightarrow c = \frac{10a - 5}{2}.$$

In conclusion,

$$f(x) = ax^2 - 5ax + \frac{10a - 5}{2}.$$

8. Let us define the quadratic function

$$f(x) = (ax_0 + b)x^2 + cx + d,$$

under the assumption $x_0 \neq -\dfrac{b}{a}$. The equation $f(x) = 0$ has real solutions because $f(x_0) = 0$, so

$$\Delta = c^2 - 4d(ax_0 + b) \geq 0 \Rightarrow x_0 \cdot 4ad \leq c^2 - 4bd \Rightarrow x_0 \leq \frac{c^2 - 4bd}{4ad}.$$

The case $x_0 = -b/a$ is trivial. Indeed, the inequality boils down to $\dfrac{c^2}{4ad} \geq 0$, which is clear.

9. Assuming that that the roots x_1, x_2 of the equation $ax^2 + bx + c = 0$ lie in $(1, 2)$, then

$$(x_1 - 1)(x_2 - 2) + (x_2 - 1)(x_1 - 2) < 0$$

$$\Rightarrow 2x_1x_2 - 3(x_1 + x_2) + 4 < 0 \Rightarrow 2 \cdot \frac{c}{a} - 3 \cdot \left(-\frac{b}{a}\right) + 4 < 0$$

$$\Rightarrow \frac{2c + 3b + 4a}{a} < 0,$$

a contradiction.

10. The conclusion is clear if $b^2 - 4ac < 0$, so assume the contrary. Let $x_1 \leq x_2$ be the real solutions of the quadratic equation $ax^2 + bx + c = 0$. For any $k \in \mathbb{Z} \cap [x_1, x_2]$, we have

$$|f(k)| < ak^2 + bk + c + 1 \leq 1 \Rightarrow |f(k)| < 1.$$

$f(k)$ is an integer, so $f(k) = 0$. Hence the interval $[x_1, x_2]$ contains at most two integers. We deduce that

$$|x_1 - x_2| < 3 \Rightarrow (x_1 - x_2)^2 < 9 \Rightarrow (x_1 + x_2)^2 - 4x_1x_2 < 9$$
$$\Rightarrow \left(-\frac{b}{a}\right)^2 - 4 \cdot \frac{c}{a} < 9 \Rightarrow b^2 - 4ac < 9a^2.$$

11. The function $g : \mathbb{R} \to \mathbb{R}$, given by the law

$$g(x) = f(x) + f(7 - x) - 7$$

is a quadratic function (possibly linear). From the inequalities

$$g(2) = f(2) + f(5) - 7 < 0 \ , \ \ g(3) = f(3) + f(4) - 7 > 0,$$

it follows that there exists $u \in (2, 3)$ for which

$$g(u) = 0 \Leftrightarrow f(u) + f(7 - u) = 7.$$

Hence it suffices to take $v = 7 - u$.

12. Denote

$$g(x) = ax^2 + bx + c, \quad h(x) = a'x^2 + b'x + c',$$

so

$$f(ax^2 + bx + c) = a'x^2 + b'x + c'.$$

For $x = 0$, $x = -b/a$, we deduce

$$f(c) = c', \quad f(c) = a'\,\frac{b^2}{a^2} - b'\,\frac{b}{a} + c',$$

so

$$a'\,\frac{b^2}{a^2} - b'\,\frac{b}{a} = 0 \Rightarrow \frac{b'}{b} = \frac{a'}{a}.$$

With $b' = mb$, $a' = ma$, we derive

$$f(ax^2 + bx + c) = m(ax^2 + bx + c) + n,$$

where $n = c' - mc$. The case $b = 0$ is similar.

13. Let $a, b, c \in \mathbb{R}$ be such that $f(x^2) = ax^2 + bx + c$, for all real numbers x. By taking $x = 1$ and $x = -1$, we deduce that $b = 0$, so $f(x^2) = ax^2 + c$ for every real number x. It follows that $f(y) = ay + c$ for all real numbers $y \in [0, \infty)$. Similarly, $f(y) = a'y + c'$ for all $y \in (-\infty, 0]$, so
$$f(y) = \begin{cases} a'y + c', & y \in (-\infty, 0] \\ ay + c, & y \in [0, \infty) \end{cases}.$$
Further, the application $x \mapsto f(x^2 + x)$ is a quadratic function. But
$$f(x^2 + x) = \begin{cases} ax^2 + ax + c, & x \in (-\infty, -1] \cup [0, \infty) \\ a'x^2 + a'x + c', & x \in [-1, 0] \end{cases},$$
so $a = a'$ and $c = c'$, hence the conclusion follows.

14. By replacing g by some function of the form $g(A + x)$, we can assume that
$$g(x) = px^2 + s, \quad f(x) = ax^2 + bx + c.$$
For any integer $k > s$, $g\left(\sqrt{\frac{k-s}{p}}\right)$ is an integer, thus $f\left(\sqrt{\frac{k-s}{p}}\right)$ is an integer. Then
$$\begin{aligned} a_k &= f\left(\sqrt{\frac{k+1-s}{p}}\right) - f\left(\sqrt{\frac{k-s}{p}}\right) \\ &= \frac{a}{p} + \frac{b}{(\sqrt{k+1-s} + \sqrt{k-s})\sqrt{p}} \in \mathbb{Z}, \end{aligned}$$
for every integer $k > s$. Because $\lim_{k \to \infty} a_k = \frac{a}{p}$ and $a_k \in \mathbb{Z}$ for all $k > s$, we have $a_k = \frac{a}{p}$ for all sufficiently large k, thus $b = 0$ and $\frac{a}{p} \in \mathbb{Z}$. The problem is now solved.

15. The function $g : [0, \infty) \to [0, \infty)$, given by the formula $g(x) = x^2 + x$ is invertible and also increasing. The given relation can be written as
$$f(g(x)) \le x \le g(f(x)).$$
By replacing first x with $g^{-1}(x)$ and from the monotony of g, we obtain that
$$\begin{aligned} f(g(x)) \le x &\Rightarrow f(x) \le g^{-1}(x) \\ g(f(x)) \ge x &\Rightarrow f(x) \ge g^{-1}(x). \end{aligned}$$
Hence
$$f(x) = g^{-1}(x) = \frac{-1 + \sqrt{1 + 4x}}{2}.$$

16. With $h(x) = f(x) - \dfrac{1}{2}$, we have

$$|h(-1)| \le 1/2, \quad |h(0)| \le 1/2, \quad |h(1)| \le 1/2.$$

We use the representation

$$h(x) = \frac{h(-1)}{2}x(x-1) + \frac{h(1)}{2}x(x+1) + h(0)(1-x^2).$$

Indeed, the application

$$x \longmapsto \frac{h(-1)}{2}x(x-1) + \frac{h(1)}{2}x(x+1) + h(0)(1-x^2)$$

is a quadratic function which coincides with the quadratic function h at $x = 0$, $x = -1$, $x = 1$. Then

$$\begin{aligned} h(x) &= \frac{h(-1)}{2}x(x-1) + \frac{h(1)}{2}x(x+1) + h(0)(1-x^2) \\ &\le \frac{1}{4}|x|(1-x) + \frac{1}{4}|x|(1+x) + \frac{1}{2}(1-x^2) \\ &= \frac{-x^2+|x|+1}{2} \le \frac{5}{8}, \end{aligned}$$

so

$$f(x) \le \frac{1}{2} + \frac{5}{8} = \frac{9}{8}.$$

17. Denote

$$f(x,y,z) = x^2 + y^2 + z^2 - xy - yz - zx.$$

We have

$$f(x,y,z) = z^2 - (x+y)z + x^2 + y^2 - xy,$$

so f is a quadratic function in z. It attains its minimum at

$$z_0 = \frac{x+y}{2} \in \left[\frac{1}{2}, \frac{3}{2}\right].$$

Consequently,

$$f(x,y,2) \le f(x,y,z) \le f(x,y,3)$$

$$\Rightarrow x^2 + y^2 - xy - 2x - 2y + 4 \le f(x,y,z) \le x^2 + y^2 - xy - 3x - 3y + 9.$$

Now, the quadratic function in x,

$$x \overset{\phi}{\longmapsto} x^2 - (y+3)x + y^2 - 3y + 9$$

attains its minimum at

$$x_0 = \frac{y+3}{2} \in \left[2, \frac{5}{2}\right],$$

so for all $x \in [0,1]$, we have

$$\phi(x) \le \phi(0) = y^2 - 3y + 9 \le 7.$$

The other side of the inequality is similar.

18. If the given equation has rational solutions, then its discriminant

$$\Delta = b^2 - 4ac$$

must be a perfect square. This is impossible, because

$$(b-1)^2 < b^2 - 4ac < b^2.$$

Indeed,

$$2b > 2a^2 + 2c^2 \ge 4ac \Rightarrow 2b > 4ac \Rightarrow 2b > 4ac + 1$$

$$\Rightarrow 2b - 1 > 4ac \Rightarrow (b-1)^2 > b^2 - 4ac.$$

19. Note that x, y satisfy the quadratic equation $t^2 - \alpha t - \beta = 0$, with $\alpha = x + y$, $\beta = -xy$, so

$$x^n = \alpha x^{n-1} + \beta x^{n-2}, \quad y^n = \alpha y^{n-1} + \beta y^{n-2}.$$

Thus

$$x^n + y^n = \alpha(x^{n-1} + y^{n-1}) + \beta(x^{n-2} + y^{n-2}).$$

According to the hypothesis,

$$\begin{cases} (a-\alpha)(x^{k-1} + y^{k-1}) + (b-\beta)(x^{k-2} + y^{k-2}) = 0 \\ (a-\alpha)(x^k + y^k) + (b-\beta)(x^{k-1} + y^{k-1}) = 0 \end{cases}.$$

If $a - \alpha \ne 0$, then $b - \beta \ne 0$ and

$$(x^{k-1} + y^{k-1})^2 = (x^k + y^k)(x^{k-2} + y^{k-2}) \Rightarrow x^{k-2}y^{k-2}(x-y)^2 = 0,$$

which is impossible. It follows that $a - \alpha = 0$ and $b - \beta = 0$, and the proof is complete.

20. If x_1, x_2 are the roots of the given equation, then

$$x_1 + x_2 = a^3 - 3a, \quad x_1 x_2 = 1.$$

With $y_1 = \sqrt[3]{x_1}$, $y_2 = \sqrt[3]{x_2}$, we have

$$\begin{aligned}(y_1 + y_2)^3 &= (\sqrt[3]{x_1} + \sqrt[3]{x_2})^3 = x_1 + x_2 + 3\sqrt[3]{x_1 x_2}(\sqrt[3]{x_1} + \sqrt[3]{x_2}) \\ &= a^3 - 3a + 3(y_1 + y_2),\end{aligned}$$

so

$$(y_1 + y_2)^3 - 3(y_1 + y_2) = a^3 - 3a$$

or

$$(y_1 + y_2 - a)\left[\left(y_1 + y_2 + \frac{a}{2}\right)^2 + \frac{3}{4}(a^2 - 4)\right] = 0,$$

which implies $y_1 + y_2 = a$. Further,

$$\sqrt[3]{x_1} + \sqrt[3]{x_2} = a \Rightarrow \sqrt[3]{x_1} + \frac{1}{\sqrt[3]{x_1}} = a \Rightarrow \sqrt[3]{x_1^2} - a\sqrt[3]{x_1} + 1 = 0.$$

Now, let us suppose that x_1 is an integer and let $u = \sqrt[3]{x_1}$. Then $u^2 - au + 1 = 0$ and $u^3 = x_1$. Thus $u^3 - au^2 + u = 0$, from which we obtain $x_1 + u = a(au - 1)$. This shows that u is a rational number. Because u^3 is an integer, u is also an integer. This shows that x_1 is the cube of a positive integer.

Chapter 8

Parametric Solutions for Certain Equations

Real equations with multiple unknowns have in general infinitely many solutions if they are solvable. In this case, one important technique is that of characterizing the set of solutions by using parameters. We are going to discuss two real equations and two parameterizations, but we will go beyond, showing how a simple idea can generate lots of nice problems, some of them really difficult.

We begin this discussion with a problem. It may seem unusual, but this problem is in fact the introduction that leads to the other themes in this discussion.

Problem. Consider three real numbers a, b, c such that $abc = 1$ and write

$$x = a + \frac{1}{a}, \quad y = b + \frac{1}{b}, \quad z = c + \frac{1}{c}. \tag{1}$$

Find an algebraic relation between x, y, z, independent of a, b, c.

Solution. Of course, without any ideas, one would solve the equations from (1) with respect to a, b, c and then substitute the results in the relation $abc = 1$. But this is a mathematical crime! Here is a nice idea. To generate a relation involving x, y, z, we compute the product

$$\begin{aligned} xyz &= \left(a + \frac{1}{a}\right)\left(b + \frac{1}{b}\right)\left(c + \frac{1}{c}\right) \\ &= \left(a^2 + \frac{1}{a^2}\right) + \left(b^2 + \frac{1}{b^2}\right) + \left(c^2 + \frac{1}{c^2}\right) + 2 \\ &= (x^2 - 2) + (y^2 - 2) + (z^2 - 2) + 2. \end{aligned}$$

Thus,

$$x^2 + y^2 + z^2 - xyz = 4 \tag{2}$$

and this is the answer to the problem.

Now, another question appears: is the converse true? Obviously not (take for example the numbers $(x, y, z) = (1, 1, -1)$). But looking again at (1), we see that we must have $\min\{|x|, |y|, |z|\} \geq 2$. We will prove the following result.

Problem. Let x, y, z be real numbers with $\max\{|x|, |y|, |z|\} > 2$ and satisfying (2). Prove that there exist real numbers a, b, c with $abc = 1$ satisfying (1).

Solution. Whenever we have a condition of the form $\max\{|x|, |y|, |z|\} > 2$, it is better to make a choice. Here, let us take $|x| > 2$. This implies that there exists a nonzero real number u such that $x = u + \frac{1}{u}$, (we have used here the condition $|x| > 2$). Now, let us regard (2) as a second degree equation with respect to z. Since this equation has real roots, the discriminant must be nonnegative, which means that $(x^2 - 4)(y^2 - 4) \geq 0$. But since $|x| > 2$, we find that $y^2 \geq 4$ and so there exists a nonzero real number v for which $y = v + \frac{1}{v}$. How do we find the corresponding z? Simply by solving the second degree equation. We find two solutions:

$$z_1 = uv + \frac{1}{uv}, \quad z_2 = \frac{u}{v} + \frac{v}{u}$$

and now we are almost done. If $z = uv + \frac{1}{uv}$, we take $(a, b, c) = \left(u, v, \frac{1}{uv}\right)$, and if $z = \frac{u}{v} + \frac{v}{u}$, then we take $(a, b, c) = \left(\frac{1}{u}, v, \frac{u}{v}\right)$. All the conditions are satisfied and the problem is solved.

A direct consequence of the previous problem is the following:

If $x, y, z > 0$ are real numbers that satisfy (2) and such that

$$\max\{|x|, |y|, |z|\} > 2,$$

then there exist $\alpha, \beta, \chi \in \mathbb{R}$ such that

$$x = 2\mathrm{ch}(\alpha), \quad y = 2\mathrm{ch}(\beta), \quad z = 2\mathrm{ch}(\chi),$$

where $\mathrm{ch} : \mathbb{R} \to (0, \infty)$, $\mathrm{ch}(x) = \frac{e^x + e^{-x}}{2}$. Indeed, we write (1), in which this time, it is clear that $a, b, c > 0$ and we take $\alpha = \ln a$, $\beta = \ln b$, $\chi = \ln c$.

Inspired by the previous equation, let us consider another one:

$$x^2 + y^2 + z^2 + xyz = 4, \tag{3}$$

where $x, y, z > 0$. We will prove that the set of solutions of this equation is the set of triples $(2\cos A, 2\cos B, 2\cos C)$ where A, B, C are the angles of an acute triangle. First, let us prove that all these triples are solutions. This reduces to the identity

$$\cos^2 A + \cos^2 B + \cos^2 C + 2\cos A \cos B \cos C = 1.$$

This identity can be proved readily by using the sum-to-product formulas, but here is a nice proof employing geometry and linear algebra. We know that in any triangle we have the relations

$$\begin{cases} a = c\cos B + b\cos C \\ b = a\cos C + c\cos A \\ c = b\cos A + a\cos B \end{cases}$$

which are simple consequences of the Law of Cosines. Now, let us consider the system

$$\begin{cases} x - y\cos C - z\cos B = 0 \\ -x\cos C + y - z\cos A = 0 \\ -x\cos B - y\cos A + z = 0 \end{cases}$$

From the above observation, it follows that this system has a nontrivial solution, that is, (a, b, c), and so we must have

$$\begin{vmatrix} 1 & -\cos C & -\cos B \\ -\cos C & 1 & -\cos A \\ -\cos B & -\cos A & 1 \end{vmatrix} = 0,$$

which, when expanded, gives

$$\cos^2 A + \cos^2 B + \cos^2 C + 2\cos A \cos B \cos C = 1.$$

For the converse, we see first that $0 < x, y, z < 2$, hence there are numbers $A, B \in \left(0, \frac{\pi}{2}\right)$ such that $x = 2\cos A$, $y = 2\cos B$. Solving the equation with respect to z and taking into account that $z \in (0, 2)$, we obtain

$$z = -2\cos(A + B).$$

Thus we can take $C = \pi - A - B$ and we will have

$$(x, y, z) = (2\cos A, 2\cos B, 2\cos C).$$

All in all, we have solved the following problem.

Problem. The positive real numbers x, y, z satisfy (3) if and only if there exists an acute-angled triangle ABC such that

$$x = 2\cos A, \quad y = 2\cos B, \quad z = 2\cos C.$$

With the introduction and the easy problems over, it is now time to see some nice applications of the above results.

Problem. Let $x, y, z > 2$ satisfy (2). We define the sequences $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$, $(c_n)_{n\geq 1}$ by

$$a_{n+1} = \frac{a_n^2 + x^2 - 4}{a_{n-1}}, \quad b_{n+1} = \frac{b_n^2 + y^2 - 4}{b_{n-1}}, \quad c_{n+1} = \frac{c_n^2 + z^2 - 4}{c_{n-1}},$$

with $a_1 = x$, $b_1 = y$, $c_1 = z$ and $a_2 = x^2 - 2$, $b_2 = y^2 - 2$, $c_2 = z^2 - 2$.

Prove that for all $n \geq 1$, the triple (a_n, b_n, c_n) also satisfies (2).

Solution. Let us write $x = a + \frac{1}{a}$, $y = b + \frac{1}{b}$, $z = c + \frac{1}{c}$, with $abc = 1$. Then

$$a_2 = a^2 + \frac{1}{a^2}, \quad b_2 = b^2 + \frac{1}{b^2}, \quad c_2 = c^2 + \frac{1}{c^2}.$$

So, a reasonable conjecture is that

$$(a_n, b_n, c_n) = \left(a^n + \frac{1}{a^n}, b^n + \frac{1}{b^n}, c^n + \frac{1}{c^n}\right).$$

Indeed, this follows by induction from

$$\frac{\left(a^n + \frac{1}{a^n}\right)^2 + a^2 + \frac{1}{a^2} - 2}{a^{n-1} + \frac{1}{a^{n-1}}} = a^{n+1} + \frac{1}{a^{n+1}}$$

and two similar identities. We have established that

$$(a_n, b_n, c_n) = \left(a^n + \frac{1}{a^n}, b^n + \frac{1}{b^n}, c^n + \frac{1}{c^n}\right).$$

But if $abc = 1$, then certainly $a^n b^n c^n = 1$, which shows that indeed, the triple (a_n, b_n, c_n) satisfies (2).

Of a different kind, the following problem and the featured solution illustrate that sometimes an efficient substitution can help more than ten complicated ideas.

Problem. Let $a, b, c > 0$. Find all triples (x, y, z) of positive real numbers such that

$$\begin{cases} x + y + z = a + b + c \\ a^2x + b^2y + c^2z + abc = 4xyz \end{cases}.$$

Solution. We try to use the information given by the second equation. This equation can be written as

$$\frac{a^2}{yz} + \frac{b^2}{zx} + \frac{c^2}{xy} + \frac{abc}{xyz} = 4,$$

and we already recognize the relation

$$u^2 + v^2 + w^2 + uvw = 4,$$

where $u = \dfrac{a}{\sqrt{yz}}$, $v = \dfrac{b}{\sqrt{zx}}$, $w = \dfrac{c}{\sqrt{xy}}$. We know that we can find an acute-angled triangle ABC such that

$$u = 2\cos A, \quad v = 2\cos B, \quad w = 2\cos C.$$

We have made use of the second condition, so we use the first one to deduce that

$$x + y + z = 2\sqrt{xy}\cos C + 2\sqrt{yz}\cos A + 2\sqrt{zx}\cos B.$$

Trying to solve this as a second degree equation in $\sqrt{x}$, after using trigonometric identities and simplifying, we find the discriminant to be

$$-4(\sqrt{y}\sin C - \sqrt{z}\sin B)^2.$$

Because this discriminant must be nonnegative, we infer that

$$\sqrt{y}\sin C = \sqrt{z}\sin B \ \text{ and } \sqrt{x} = \sqrt{y}\cos C + \sqrt{z}\cos B.$$

Now we use the fact that

$$\cos A = \frac{a}{2\sqrt{yz}}, \quad \cos B = \frac{b}{2\sqrt{zx}}, \quad \cos C = \frac{c}{2\sqrt{xy}},$$

and we find

$$\sqrt{x} = \sqrt{y}\cos C + \sqrt{z}\cos B = \sqrt{y}\cdot\frac{c}{2\sqrt{xy}} + \sqrt{z}\cdot\frac{b}{2\sqrt{zx}} = \frac{1}{\sqrt{x}}\cdot\frac{b+c}{2},$$

that is $x = (b+c)/2$.

We proceed in a similar manner for y and z, and we get the conclusion:

$$x = \frac{b+c}{2}, \quad y = \frac{c+a}{2}, \quad z = \frac{a+b}{2}.$$

It is immediate to see that this triple satisfies both conditions, hence there is a unique solution (the above one) to the given system.

Notice that we almost proved the inequality

$$x + y + z \geq 2\sqrt{xy}\cos C + 2\sqrt{yz}\cos A + 2\sqrt{zx}\cos B,$$

valid for all positive x, y, and z and for any A, B, and C representing the measures of the angles of a triangle. The equality

$$x + y + z = 2\sqrt{xy}\cos C + 2\sqrt{yz}\cos A + 2\sqrt{zx}\cos B$$

occurs if and only if

$$\frac{\sqrt{x}}{\sin A} = \frac{\sqrt{y}}{\sin B} = \frac{\sqrt{z}}{\sin C}.$$

We invite the reader to fill in the details of a complete proof.

Proposed Problems

1. Solve in the set of positive real numbers the system
$$\begin{cases} x^2+y^2+z^2+xyz=4 \\ x+y+z=3 \end{cases}.$$

2. Let x, y, z be positive reals such that $x^2+y^2+z^2+xyz=4$. Prove that
$$\sqrt{\frac{(2-x)(2-y)}{(2+x)(2+y)}}+\sqrt{\frac{(2-y)(2-z)}{(2+y)(2+z)}}+\sqrt{\frac{(2-z)(2-x)}{(2+z)(2+x)}}=1.$$

3. Find all triples (k, l, m) of real numbers with $k+l+m=2002$ for which the system
$$\begin{cases} \dfrac{x}{y}+\dfrac{y}{x}=k \\ \dfrac{y}{z}+\dfrac{z}{y}=l \\ \dfrac{z}{x}+\dfrac{x}{z}=m \end{cases}$$
has solutions in the set of real numbers.

4. Let x, y, z be positive real numbers such that $x+y+z=xyz$. Prove that
$$\frac{1}{1+x^2}+\frac{1}{1+y^2}+\frac{1}{1+z^2}+\frac{2}{\sqrt{(1+x^2)(1+y^2)(1+z^2)}}=1.$$

5. Let a, b, c be positive reals such that $a+b+c+2\sqrt{abc}=1$. Prove that
$$\sqrt{\frac{1-a}{a}}+\sqrt{\frac{1-b}{b}}+\sqrt{\frac{1-c}{c}}=\sqrt{\frac{1-a}{a}}\cdot\sqrt{\frac{1-b}{b}}\cdot\sqrt{\frac{1-c}{c}}.$$

6. Prove that the equation $x^2+y^2+z^2+xyz=4$ has infinitely many solutions in integers.

7. Let $(a_n)_{n\in\mathbb{N}}$ be a strictly increasing sequence of real numbers satisfying
$$a_{n+1}^2+a_n^2+a_{n-1}^2-a_{n+1}a_na_{n-1}=4,$$
for all positive integers n, with $a_0=a_1=47$. Prove that:

a) $2+a_n$ is a square for every $n\in\mathbb{N}$;

b) $2+\sqrt{2+a_n}$ is a square for every $n\in\mathbb{N}$.

8. Let a, b, c be nonnegative real numbers such that
$$a^2 + b^2 + c^2 + abc = 4.$$
Prove that $0 \leq ab + bc + ca - abc \leq 2$.

9. Let a, b, c be nonnegative real numbers such that $x^2+y^2+z^2+2xyz = 1$. Prove that $xyz \leq 1/8$.

10. Let x, y, z be positive real numbers fulfilling the condition
$$x^2 + y^2 + z^2 = xyz.$$
Prove that the inequality
$$xy + xz + yz \geq 4\,(x + y + z) - 9$$
holds.

11. Prove that for any positive real numbers x, y, z satisfying
$$x + y + z = xyz,$$
the inequality
$$(x-1)(y-1)(z-1) \leq 6\sqrt{3} - 10$$
holds.

Solutions

1. Let us consider the acute-angled triangle ABC for which
$$x = 2\cos A, \quad y = 2\cos B, \quad z = 2\cos C.$$
Then the second equation of the system becomes
$$\cos A + \cos B + \cos C = \frac{3}{2},$$
so the triangle ABC is equilateral. Thus, $x = y = z = 1$.

2. Let $A, B, C \in [0, \pi/2)$ be such that $A + B + C = \pi$ and
$$x = 2\cos A, \quad y = 2\cos B, \quad z = 2\cos C.$$
Then with
$$\frac{2-x}{2+x} = \frac{2-2\cos A}{2+2\cos A} = \frac{1-\cos A}{1+\cos A} = \frac{2\sin^2\frac{A}{2}}{2\cos^2\frac{A}{2}} = \tan^2\frac{A}{2},$$

one obtains

$$\sqrt{\frac{(2-x)(2-y)}{(2+x)(2+y)}}+\sqrt{\frac{(2-y)(2-z)}{(2+y)(2+z)}}+\sqrt{\frac{(2-z)(2-x)}{(2+z)(2+x)}}$$

$$=\tan\frac{A}{2}\tan\frac{B}{2}+\tan\frac{B}{2}\tan\frac{C}{2}+\tan\frac{C}{2}\tan\frac{A}{2}=1,$$

which is an identity.

3. As we have already proved,

$$k^2+l^2+m^2-4=klm,$$

and by adding $2kl+2lm+2mk$, we obtain

$$klm+2kl+2lm+2mk+4=(k+l+m)^2,$$

and by adding $4(k+l+m)+4$,

$$(k+2)(l+2)(m+2)=(k+l+m+2)^2$$

or

$$(k+2)(l+2)(m+2)=2004^2=2^4\cdot 3^2\cdot 167^2.$$

The factor 167 can occur with exponent greater than 1 in the factorization of neither of $k+2$, $l+2$, or $m+2$, because the sum

$$(k+2)+(l+2)+(m+2)=2008,$$

and 167^2 is much greater than 2008. So two of these numbers have the factor 167, say 167 divides $k+2$ and $l+2$. Then

$$167\left(\frac{k+2}{167}+\frac{l+2}{167}\right)+(m+2)=2008$$

and

$$\frac{k+2}{167}\cdot\frac{l+2}{167}\cdot(m+2)=2^4\cdot 3^2.$$

Now we cannot have

$$\frac{k+2}{167}+\frac{l+2}{167}\geq 13$$

because $167\cdot 13>2008$, and we cannot have

$$\frac{k+2}{167}+\frac{l+2}{167}\leq 11$$

because $m+2$ can be at most $2^4 \cdot 3^2 = 144$, and $167 \cdot 11 + 144 < 2008$. Thus, necessarily,

$$\frac{k+2}{167} + \frac{l+2}{167} = 12$$

and, because $(k+2)/167$ and $(l+2)/167$ are factors of $2^4 \cdot 3^2$ we see that the only possibility is

$$\frac{k+2}{167} = \frac{l+2}{167} = 6.$$

Taking into account the symmetry of the equations satisfied by k, l, and m, we see that the triples (k, l, m) can only be

$$(2, 1000, 1000)\,, \quad (1000, 2, 1000)\,, \quad (1000, 1000, 2)\,.$$

For these values, the given system has solutions

$$\begin{gathered}\left(1, 500 + \sqrt{500^2 - 1}, 500 + \sqrt{500^2 - 1}\right)\\ \left(500 + \sqrt{500^2 - 1}, 1, 500 + \sqrt{500^2 - 1}\right)\\ \left(500 + \sqrt{500^2 - 1}, 500 + \sqrt{500^2 - 1}, 1\right).\end{gathered}$$

4. We prove that there exist $A, B, C \in [0, \pi/2)$ with $A + B + C = \pi$ and

$$x = \tan A, \quad y = \tan B, \quad z = \tan C.$$

Let $A, B \in [0, \pi/2)$ be such that $x = \tan A$, $y = \tan B$. Then from the given equation,

$$z = -\frac{x+y}{1-xy} = -\frac{\tan A + \tan B}{1 - \tan A \tan B} = -\tan(A+B) = \tan C,$$

where $C = \pi - A - B$. Now,

$$\frac{1}{1+x^2} = \frac{1}{1+\tan^2 A} = \cos^2 A,$$

and similar equations result for y and z. Finally,

$$\frac{1}{1+x^2} + \frac{1}{1+y^2} + \frac{1}{1+z^2} + \frac{2}{\sqrt{(1+x^2)(1+y^2)(1+z^2)}}$$

$$= \cos^2 A + \cos^2 B + \cos^2 C + 2\cos A \cos B \cos C = 1,$$

which is an identity.

5. We have

$$(2\sqrt{a})^2+(2\sqrt{b})^2+(2\sqrt{c})^2+(2\sqrt{a})(2\sqrt{b})(2\sqrt{c})=4,$$

so

$$\sqrt{a}=\cos A,\quad \sqrt{b}=\cos B,\quad \sqrt{c}=\cos C,$$

for some $A, B, C \in [0,\pi/2)$ with $A+B+C=\pi$. Then

$$\sqrt{\frac{1-a}{a}}=\sqrt{\frac{1-\cos^2 A}{\cos^2 A}}=\tan A,$$

and analogous equations follow for b and c. The requested relation becomes

$$\tan A+\tan B+\tan C=\tan A\tan B\tan C,$$

which is an identity.

6. Let us order the equation with respect to z,

$$z^2+xyz+x^2+y^2-4=0.$$

If we want integer solutions, then we must have the discriminant

$$\Delta=(x^2-4)(y^2-4)$$

a square. It is a square if, for example, $x=y$. In that case,

$$z^2+x^2z+2x^2-4=0$$

with $\sqrt{\Delta}=\left|x^2-4\right|$. Then

$$z=\frac{-x^2\pm(x^2-4)}{2}.$$

We have found an infinite number of solutions,

$$(x,x,-2),\quad \left(x,x,2-x^2\right),$$

for every integer x.

7. We have seen in a problem solved in the theoretical part, that the equation

$$x^2+\left(a+\frac{1}{a}\right)^2+\left(b+\frac{1}{b}\right)^2-\left(a+\frac{1}{a}\right)\left(b+\frac{1}{b}\right)x=4$$

has solutions

$$x_1 = ab + \frac{1}{ab} \text{ and } x_2 = \frac{a}{b} + \frac{b}{a}.$$

One immediately sees that if $a \geq b > 1$, then

$$ab + \frac{1}{ab} > a + \frac{1}{a} > \frac{a}{b} + \frac{b}{a}.$$

(Indeed, the first inequality is equivalent to $(ab-1)(b-1) > 0$, and the second transforms into $(a^2 - b)(b-1) > 0$, and we have $b - 1 > 0$, $a^2b - 1 > 1 - 1 = 0$, and $a^2 > a \geq b$, hence $a^2 - b > 0$.)

We have

$$a_0 = a_1 = 47 = \alpha + \frac{1}{\alpha}$$

with $\alpha = (47 + 21\sqrt{5})/2 > 1$. By replacing in

$$a_2^2 + a_1^2 + a_0^2 - a_2a_1a_0 = 4$$

we find that $a_2 = 2$, or $a_2 = 47^2 - 2$. Thus, because the sequence is increasing,

$$a_2 = 47^2 - 2 = \alpha^2 + \frac{1}{\alpha^2}.$$

Now it seems reasonable to conjecture that

$$a_n = b_n + \frac{1}{b_n},$$

with $(b_n)_{n\in\mathbb{N}}$ an increasing sequence of real numbers, all greater than 1. And this follows inductively, since, if the result is true for $n-1$ and n, then a_{n+1} is the solution of the equation

$$x^2 + \left(b_n + \frac{1}{b_n}\right)^2 + \left(b_{n-1} + \frac{1}{b_{n-1}}\right)^2 - \left(b_n + \frac{1}{b_n}\right)\left(b_{n-1} + \frac{1}{b_{n-1}}\right)x = 4$$

which is greater than a_n. According to the above observations, we have two solutions for this equation, namely

$$b_nb_{n-1} + \frac{1}{b_nb_{n-1}} \text{ and } \frac{b_n}{b_{n-1}} + \frac{b_{n-1}}{b_n},$$

and yet we know that

$$b_nb_{n-1} + \frac{1}{b_nb_{n-1}} > b_n + \frac{1}{b_n} > \frac{b_n}{b_{n-1}} + \frac{b_{n-1}}{b_n},$$

that is, only the first one is greater than a_n. Consequently, we must have

$$a_{n+1} = b_n b_{n-1} + \frac{1}{b_n b_{n-1}},$$

or

$$a_{n+1} = b_{n+1} + \frac{1}{b_{n+1}},$$

with $b_{n+1} = b_n b_{n-1} > b_n$.

Because, as we have seen, $b_0 = b_1 = \alpha$ and $b_{n+1} = b_n b_{n-1}$ for all $n \in \mathbb{N}$, it follows immediately that $b_n = \alpha^{F_n}$, where $(F_n)_{n\in\mathbb{N}}$ is the Fibonacci sequence (defined by $F_0 = F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for all $n \geq 1$). Finally, it is not hard to see that $\alpha = \beta^4$, with

$$\beta = \frac{3+\sqrt{5}}{2},$$

therefore we actually have

$$a_n = \beta^{4F_n} + \frac{1}{\beta^{4F_n}},$$

for all n. Yet

$$\beta^{k+1} + \frac{1}{\beta^{k+1}} = 3\left(\beta^k + \frac{1}{\beta^k}\right) - \left(\beta^{k-1} + \frac{1}{\beta^{k-1}}\right)$$

for all $k \geq 1$ (verify this!) allows us to prove by a standard inductive argument that $\beta^k + \beta^{-k}$ is an integer for all $k \in \mathbb{N}$ (actually a positive integer). It remains to see that

$$2 + a_n = 2 + \beta^{4F_n} + \frac{1}{\beta^{4F_n}} = \left(\beta^{2F_n} + \frac{1}{\beta^{2F_n}}\right)^2$$

is a square, and that

$$2 + \sqrt{2 + a_n} = 2 + \beta^{2F_n} + \frac{1}{\beta^{2F_n}} = \left(\beta^{F_n} + \frac{1}{\beta^{F_n}}\right)^2$$

is a square, too, thus finishing the proof.

8. The three numbers cannot be all greater than 1, otherwise we get the contradiction

$$4 = a^2 + b^2 + c^2 + abc > 1 + 1 + 1 + 1 + 1 = 4.$$

(For a similar reason, a, b, and c cannot be all less than 1.) Thus we may assume, for example, $c \leq 1$. We then have

$$ab + bc + ca - abc = ab(1 - c) + bc + ca \geq 0,$$

and the first inequality is proved.

Now, from the three numbers there must be two that are both at least equal to 1, or both at most 1. If a and b are those we have

$$(1 - a)(1 - b) \geq 0.$$

On the other hand, the given condition and the AM-GM inequality yield

$$2ab + c^2 + abc \leq a^2 + b^2 + c^2 + abc = 4 \Leftrightarrow ab(2 + c) \leq (2 - c)(2 + c),$$

hence $ab \leq 2 - c$, or $ab + c \leq 2$. We thus have

$$ab + bc + ca - abc = ab + c - c(1 - a)(1 - b) \leq ab + c \leq 2,$$

and we are done with the second inequality, too.

Note that (when a, b, and c are positive) we have

$$a = 2\cos A, \quad b = 2\cos B, \quad c = 2\cos C,$$

for some $A, B, C \in [0, \pi/2)$ with $A + B + C = \pi$. Thus we have the inequalities

$$0 \leq \cos A + \cos B + \cos C - 2\cos A \cos B \cos C \leq \frac{1}{2}$$

in any acute triangle. The reader can check that equality holds in the second inequality for equilateral triangles only, and it is not achievable in the first inequality. (Or we can consider that it is achievable, but only for a "triangle" with two right angles.)

9. Multiplying by 4, we obtain

$$(2x)^2 + (2y)^2 + (2z)^2 + (2x)(2y)(2z) = 4,$$

so

$$x = \cos A, \quad y = \cos B, \quad z = \cos C$$

for some $A, B, C \in [0, \pi/2)$ with $A + B + C = \pi$. The conclusion follows if we take into account that in every triangle ABC, we have

$$\cos A \cos B \cos C \leq \frac{1}{8}.$$

We also can prove the result using purely algebraic methods. Indeed, let us assume, by way of contradiction, that

$$xyz > \frac{1}{8}.$$

Then, by the geometric-quadratic mean inequality, we deduce that

$$\sqrt{\frac{x^2 + y^2 + z^2}{3}} \geq \sqrt[3]{xyz} > \frac{1}{2}$$

and thus

$$x^2 + y^2 + z^2 > \frac{3}{4}.$$

From here,

$$1 = x^2 + y^2 + z^2 + 2xyz > \frac{3}{4} + 2 \cdot \frac{1}{8} = 1,$$

which is false.

10. We immediately get $z > 2$ from the given condition, since

$$xyz = x^2 + y^2 + z^2 > 2xy;$$

$x > 2$ and $y > 2$ follow analogously. Thus let

$$x - 2 = a, \quad y - 2 = b, \quad z - 2 = c,$$

for which $a > 0$, $b > 0$, $c > 0$ and, of course, $x = a+2$, $y = b+2$, $z = c+2$. By replacing in the given condition, we obtain

$$(a+2)^2 + (b+2)^2 + (c+2)^2 = (a+2)(b+2)(c+2)$$
$$\Leftrightarrow a^2 + b^2 + c^2 + 4 = abc + 2(ab + ac + bc),$$

after simple computations.

Now, using well-known inequalities, we have

$$ab + ac + bc + 4 \leq a^2 + b^2 + c^2 + 4 = abc + 2(ab + ac + bc)$$
$$\leq \left(\frac{ab + ac + bc}{3}\right)^{3/2} + 2(ab + ac + bc),$$

whence, if we denote $t = \sqrt{3(ab + ac + bc)}$,

$$\frac{t^3}{27} + \frac{t^2}{3} \geq 4$$

follows. But this can be rewritten as

$$(t-3)(t+6)^2 \geq 0,$$

yielding

$$\sqrt{3(ab+ac+bc)} = t \geq 3 \Rightarrow ab+ac+bc \geq 3.$$

All that remains is to rewrite this in terms of the variables x, y, z:

$$(x-2)(y-2)+(x-2)(z-2)+(y-2)(z-2) \geq 3$$

$$\Leftrightarrow xy+xz+yz \geq 4(x+y+z)-9,$$

thus getting precisely the desired inequality.

Remark. Let ABC be a triangle with lengths of its sides a, b, and c, and semiperimeter s. Also, let

$$M = \sqrt{\tan(A/2)\tan(B/2)\tan(C/2)}.$$

Show that if x, y, and z fulfill the given condition, we can give them either of the parametric forms

$$x = \frac{s}{\sqrt{(s-b)(s-c)}}, \quad y = \frac{s}{\sqrt{(s-a)(s-c)}}, \quad z = \frac{s}{\sqrt{(s-a)(s-b)}},$$

or

$$x = \frac{1}{M\sqrt{\tan(A/2)}}, \quad y = \frac{1}{M\sqrt{\tan(B/2)}}, \quad z = \frac{1}{M\sqrt{\tan(C/2)}}$$

These parameterizations lead to interesting geometric forms of the given inequality.

11. Since the numbers are positive, from the given condition, it follows immediately that $x < xyz \Leftrightarrow yz > 1$, and similarly $xz > 1$ and $yz > 1$, thus it is not possible for two of the numbers to be less than or equal to 1. If one number is less than 1 and two are greater than 1, the inequality is obviously true (the product from the left-hand side being negative), so we consider the case when $x > 1, y > 1, z > 1$. Then the numbers $u = x-1, v = y-1$ and $w = z-1$ are positive and, replacing $x = u+1, y = v+1, w = z+1$ in the condition from the hypothesis, we obtain

$$uvw + uv + uw + vw = 2.$$

By the inequality between the arithmetic mean and geometric mean of three positive numbers, we obtain

$$uvw + 3\sqrt[3]{u^2v^2w^2} \leq uvw + uv + uw + vw = 2,$$

hence for $t = \sqrt[3]{uvw}$, we have

$$t^3 + 3t^2 - 2 \le 0 \Leftrightarrow (t+1)(t+1+\sqrt{3})(t+1-\sqrt{3}) \le 0.$$

From here, $t \le \sqrt{3} - 1$ follows, yielding the desired inequality

$$uvw = t^3 \le (\sqrt{3}-1)^3 = 6\sqrt{3} - 10.$$

The only equality case occurs when each of x, y, and z equals $\sqrt{3}$.

Remarks. 1) The unconditioned form of the inequality is

$$(x+y+z)\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right) - 9 \ge \frac{2(x+y+z)\sqrt{x+y+z}}{\sqrt{xyz}} - 6\sqrt{3},$$

for all positive x, y, and z.

2) If we parameterize with $x = \cot(A/2)$, $y = \cot(B/2)$ and $z = \cot(C/2)$ (with A, B, and C being the angles of a triangle), we get the celebrated inequality of Blundon:

$$s \le 2R + (3\sqrt{3} - 4)r$$

(with the usual notations in a triangle: s is the semiperimeter, R and r are the circumradius and inradius, respectively). For details, see the article *An Elementary Proof of Blundon's Inequality* by Gabriel Dospinescu, Mircea Lascu, Cosmin Pohoaţă, and one of the authors of this book, in *Journal of Inequalities in Pure and Applied Mathematics*, 4/2008.

3) One can use the inequality from the problem to prove that

$$h_a + h_b + h_c - 9r \ge 2s\sqrt{\frac{2r}{R}} - 6\sqrt{3}r$$

holds in any triangle, where s, R, and r have the same meaning as above, while h_a, h_b, and h_c are the lengths of triangle's altitudes. See also problem 11330 from *The American Mathematical Monthly*, 10/2007.

Chapter 9

The Scalar Product

The scalar product of two vectors $\overrightarrow{u}$, $\overrightarrow{v}$, denoted $\overrightarrow{u} \cdot \overrightarrow{v}$, is the real number obtained by multiplying the lengths of the given vectors by the cosine of the angle between them,

$$\overrightarrow{u} \cdot \overrightarrow{v} = u \cdot v \cdot \cos\alpha,$$

where $\alpha = \angle(\overrightarrow{u}, \overrightarrow{v})$. A direct consequence of this definition is the following useful property: if $\overrightarrow{u}$, $\overrightarrow{v}$ are nonzero vectors, then

$$\overrightarrow{u} \cdot \overrightarrow{v} = 0 \Leftrightarrow \overrightarrow{u} \perp \overrightarrow{v}.$$

Further, $\overrightarrow{u} \cdot \overrightarrow{u} = u^2$. The scalar product is commutative:

$$\overrightarrow{u} \cdot \overrightarrow{v} = \overrightarrow{v} \cdot \overrightarrow{u},$$

distributive with respect to addition:

$$\overrightarrow{u} \cdot (\overrightarrow{v} + \overrightarrow{w}) = \overrightarrow{u} \cdot \overrightarrow{v} + \overrightarrow{u} \cdot \overrightarrow{w},$$

and for every real number λ,

$$\lambda(\overrightarrow{u} \cdot \overrightarrow{v}) = (\lambda\overrightarrow{u}) \cdot \overrightarrow{v} = \overrightarrow{u} \cdot (\lambda\overrightarrow{v}).$$

One can easily prove that the scalar product of two vectors is the product between the length of one of them and the projection of the other vector on the first vector's direction.

Problem. (Euler) Let E, F be the midpoints of the diagonals AC and BD of the quadrilateral $ABCD$. Prove the equality

$$AC^2 + BD^2 = AB^2 + BC^2 + CD^2 + DA^2 - 4EF^2.$$

Solution I. Let us denote $\overrightarrow{a} = \overrightarrow{AB}$, $\overrightarrow{b} = \overrightarrow{BC}$, $\overrightarrow{c} = \overrightarrow{CD}$. Then

$$\overrightarrow{AC} = \overrightarrow{a} + \overrightarrow{b},\ \overrightarrow{BD} = \overrightarrow{b} + \overrightarrow{c},\ \text{and}\ \overrightarrow{AD} = \overrightarrow{a} + \overrightarrow{b} + \overrightarrow{c}.$$

Further,

$$\overrightarrow{AF} = \frac{1}{2}\left(\overrightarrow{AB} + \overrightarrow{AD}\right) = \frac{1}{2}\left(2\vec{a} + \vec{b} + \vec{c}\right),$$

$$\overrightarrow{AE} = \frac{1}{2}\overrightarrow{AC} = \frac{1}{2}\left(\vec{a} + \vec{b}\right),$$

so

$$\overrightarrow{EF} = \overrightarrow{AF} - \overrightarrow{AE} = \frac{1}{2}\left(\vec{a} + \vec{c}\right).$$

Now,

$$\begin{aligned} AC^2 + BD^2 &= \left(\vec{a} + \vec{b}\right)^2 + \left(\vec{b} + \vec{c}\right)^2 \\ &= \left(a^2 + 2\vec{a}\,\vec{b} + b^2\right) + \left(b^2 + 2\,\vec{b}\,\vec{c} + c^2\right) \\ &= a^2 + 2b^2 + c^2 + 2\vec{a}\,\vec{b} + 2\,\vec{b}\,\vec{c}. \end{aligned} \tag{1}$$

On the other hand,

$$\begin{aligned} &AB^2 + BC^2 + CD^2 + DA^2 - 4EF^2 \\ &= a^2 + b^2 + c^2 + \left(\vec{a} + \vec{b} + \vec{c}\right)^2 - \left(\vec{a} + \vec{c}\right)^2 \\ &= a^2 + b^2 + c^2 + a^2 + b^2 + c^2 + 2\vec{a}\,\vec{b} + 2\,\vec{b}\,\vec{c} + 2\vec{c}\,\vec{a} - \left(a^2 + c^2 + 2\vec{a}\,\vec{c}\right) \\ &= a^2 + 2b^2 + c^2 + 2\vec{a}\,\vec{b} + 2\,\vec{b}\,\vec{c}. \end{aligned} \tag{2}$$

The conclusion follows from (1) and (2).

Solution II. You might find this approach more convenient. We have $\overrightarrow{EF} = \overrightarrow{EA} + \overrightarrow{AD} + \overrightarrow{DF}$, and, similarly, $\overrightarrow{EF} = \overrightarrow{EC} + \overrightarrow{CB} + \overrightarrow{BF}$. Summing up these two equalities, and keeping in mind that E and F are the midpoints of the diagonals, we get $2\overrightarrow{EF} = \overrightarrow{AD} + \overrightarrow{CB}$. By squaring, we get

$$4EF^2 = AD^2 + BC^2 + 2\overrightarrow{AD} \cdot \overrightarrow{CB}.$$

Now use

$$YZ^2 = XY^2 + XZ^2 - 2\overrightarrow{XY} \cdot \overrightarrow{XZ} \Leftrightarrow 2\overrightarrow{XY} \cdot \overrightarrow{XZ} = XY^2 + XZ^2 - YZ^2$$

for any points X, Y, and Z (which is actually the cosine law — as a moment of thinking shows — and can be immediately obtained by squaring $\overrightarrow{YZ} = \overrightarrow{XZ} - \overrightarrow{XY}$) to evaluate

$$\begin{aligned} 2\overrightarrow{AD} \cdot \overrightarrow{CB} &= 2\overrightarrow{AD} \cdot \overrightarrow{AB} - 2\overrightarrow{AD} \cdot \overrightarrow{AC} \\ &= \left(AD^2 + AB^2 - BD^2\right) - \left(AD^2 + AC^2 - CD^2\right) \\ &= AB^2 + CD^2 - AC^2 - BD^2, \end{aligned}$$

and replace this in the above expression of $4EF^2$ in order to finish the proof.

Note that there is no need for $ABCD$ to be a quadrilateral, with AC and BD as diagonals, but rather, A, B, C, and D may be any points in the (three dimensional) space, with E and F the midpoints of AC and BD. (Similar expressions can be found for the square of the length of the line segment joining the midpoints of AD and BC or the midpoints of AB and CD. For instance, if M and N are the midpoints of AD and BC, respectively, then

$$4MN^2 = AB^2 + CD^2 + AC^2 + BD^2 - AD^2 - CB^2,$$

and the proof is basically the same.) However, we preferred the classical wording, which is due to (anyway, mostly named after) Euler. Euler's result generalizes a much older result of Apollonius which states that the sum of the squares of lengths of the sides of a parallelogram equals the sum of the squares of the lengths of its diagonals — so that it is known as Apollonius's theorem. A further generalization goes as follows: if A, B, C, D are points in space and P and Q are defined by the vectorial equalities $\overrightarrow{PA} = k\overrightarrow{PC}$, and $\overrightarrow{QB} = k\overrightarrow{QD}$ (where $k \neq 1$ is some real number), then

$$(1-k)^2PQ^2 = AB^2 + k^2CD^2 - kAD^2 - kBC^2 + kAC^2 + kBD^2.$$

Of course, this one misses the symmetry of the particular case $k = -1$, and loses a lot in the realm of beauty. Moreover, it brings no new methods of proof; it is just a little bit more general (the result, not its proof). We consider it a good exercise for the reader who wants to practice.

Problem. Let $ABCD$ be a quadrilateral. Prove that the diagonals AC and BD are perpendicular if and only if

$$AB^2 + CD^2 = AD^2 + BC^2.$$

Solution I. Let us denote $\overrightarrow{a} = \overrightarrow{AB}$, $\overrightarrow{b} = \overrightarrow{BC}$, $\overrightarrow{c} = \overrightarrow{CD}$, so

$$\overrightarrow{AD} = \overrightarrow{a} + \overrightarrow{b} + \overrightarrow{c}.$$

We have

$$\begin{aligned}
&AB^2 + CD^2 = AD^2 + BC^2\\
\Leftrightarrow\ & a^2 + c^2 = \left(\overrightarrow{a} + \overrightarrow{b} + \overrightarrow{c}\right)^2 + b^2\\
\Leftrightarrow\ & a^2 + c^2 = a^2 + 2b^2 + c^2 + 2\overrightarrow{a}\,\overrightarrow{b} + 2\,\overrightarrow{b}\,\overrightarrow{c} + 2\overrightarrow{c}\,\overrightarrow{a}\\
\Leftrightarrow\ & b^2 + \overrightarrow{a}\,\overrightarrow{b} + \overrightarrow{b}\,\overrightarrow{c} + \overrightarrow{c}\,\overrightarrow{a} = 0\\
\Leftrightarrow\ & \left(\overrightarrow{a} + \overrightarrow{b}\right)\left(\overrightarrow{b} + \overrightarrow{c}\right) = 0\\
\Leftrightarrow\ & \overrightarrow{AC} \cdot \overrightarrow{BD} = 0 \Leftrightarrow AC \perp BD.
\end{aligned}$$

Solution II. Or, alternatively, use again

$$2\overrightarrow{XY}\cdot\overrightarrow{XZ} = XY^2 + XZ^2 - YZ^2$$

to express

$$2\overrightarrow{AC}\cdot\overrightarrow{BD} = AD^2 + BC^2 - AB^2 - CD^2$$

(exactly as above) for a very quick proof. Again, note that A, B, C, and D need not be the vertices of a quadrilateral with diagonals AC and BD. They can be any points in space, and the problem says that the perpendicularity of AC and BD is equivalent to $AB^2 + CD^2 = AD^2 + BC^2$.

Problem. Let B, C, and D be collinear points such that D lies between B and C, and let A be any other point. Prove Stewart's theorem, namely that

$$AB^2\cdot CD - AD^2\cdot BC + AC^2\cdot BD = BC\cdot BD\cdot CD.$$

Solution. Let $r = BD/BC$, so that $1 - r = CD/BC$, and

$$(1-r)\overrightarrow{BD} + r\overrightarrow{CD} = \overrightarrow{0}.$$

We can rewrite the last equation as

$$(1-r)(\overrightarrow{AD} - \overrightarrow{AB}) + r(\overrightarrow{AD} - \overrightarrow{AC}) = \overrightarrow{0}$$

and thus $\overrightarrow{AD} = (1-r)\overrightarrow{AB} + r\overrightarrow{AC}$ follows. By squaring, we get

$$\begin{aligned} AD^2 &= (1-r)^2AB^2 + r^2AC^2 + 2r(1-r)\overrightarrow{AB}\cdot\overrightarrow{AC} \\ &= (1-r)^2AB^2 + r^2AC^2 + r(1-r)(AB^2 + AC^2 - BC^2) \\ &= (1-r)AB^2 + rAC^2 - r(1-r)BC^2. \end{aligned}$$

Now just replace $1 - r$ and r with who they really are in order to obtain the desired identity.

By the way, Stewart's theorem turns out to be a very useful tool for computing the lengths of cevians in terms of lengths of sides of triangles. For example, when D is the midpoint of the line segment BC, Stewart's theorem gives (after very little calculation)

$$4AD^2 = 2(AB^2 + AC^2) - BC^2,$$

that is, the length of the median of triangle ABC in terms of its side lengths (also known as the theorem of median). Check (it is easy) that this is equivalent to the aforementioned theorem of Apollonius about parallelograms! Also try to compute the length of the angle bisector of a triangle (either interior, or exterior) with the help of Stewart's theorem (use the fact that

$BD/CD = AB/AC$ in order to find the lengths of BD and DC in terms of AB, AC, and BC), or the length of the symmedian (in this case, use Steiner's theorem, that is, the fact that $BD/CD = (AB/AC)^2$).

The scalar product also appears quite naturally in problems that do not have (at least at first glance) a geometric statement. Consider for instance the following problem, whose solution using scalar products is straightforward, but which wouldn't be so easy using another approach.

Problem. Let a, b, c, d, e, f, g, h be real numbers. Prove that the following numbers

$$ac + bd,\ ae + bf,\ ag + bh,\ ce + df,\ cg + dh,\ eg + fh$$

cannot be all negative.

Solution. Let us consider the vectors (a, b), (c, d), (e, f), (g, h) in a rectangular system OXY. We can find two vectors, say (a, b) and (c, d), such that the angle between them is either acute or 90°. Consequently, the scalar product $(a, b) \cdot (c, d) = ac + bd$ is nonnegative.

Proposed Problems

1. Prove the altitude to the hypotenuse theorem (the right triangle altitude theorem) by using the scalar product.

2. Let $ABCD$ be a square, and let M and N be the midpoints of AB and BC, respectively. Prove that the lines DM and AN are perpendicular.

3. Let ABC be a right triangle with $m(\angle BAC) = 90^\circ$ and $m(\angle ACB) = 30^\circ$. Let D be the midpoint of BC and let E be on the line segment AC such that $AC = 3AE$. Prove that AD and BE are perpendicular.

4. Let ABC be a right triangle with $m(\angle BAC) = 90^\circ$ and let AD be its altitude from A ($D \in BC$). Let M and N be the midpoints of AD and BD, respectively. Prove that AN and CM are perpendicular.

5. Let A, B, C, and D be arbitrary points in space, and let M, N, P, and Q be the midpoints of AB, CD, AC, and BD, respectively. Prove that MN and PQ are perpendicular if and only if $AD = BC$.

6. Let $ABCD$ be a quadrilateral (or a tetrahedron) and let K, L, M, N be the midpoints of the sides (respectively edges) AB, BC, CD, DA. Prove the equality

   $$(AB^2 + CD^2) - (AD^2 + BC^2) = 2(LN^2 - KM^2) = 2AC \cdot BD \cdot \cos\alpha,$$

   where α is the angle between vectors $\overrightarrow{AC}$ and $\overrightarrow{DB}$.

7. Let H be the orthocenter of the acute triangle ABC and let $A' \in (HA$, $B' \in (HB$, $C' \in (HC$ (where by $(XY$ we mean the ray that emerges from X and contains Y) be such that $HA' = BC$, $HB' = CA$, $HC' = AB$. Prove that the sides of the triangle $A'B'C'$ are perpendicular to the medians of the triangle ABC.

8. Let $ABCDEF$ be a convex hexagon and let M, N, P, Q, R, S be the respective midpoints of the sides AB, BC, CD, DE, EF, FA. Prove that $MQ \perp PS$ if and only if
$$RN^2 = MQ^2 + PS^2.$$

9. Let ABC be a triangle. Denote by O the circumcenter, D the midpoint of side AB, and E the centroid of the triangle ACD. Prove that $OE \perp CD$ if and only if $AB = AC$.

10. Let ABC and $A'B'C'$ be given triangles. Prove that if the perpendicular lines from A, B, C onto $B'C', C'A', A'B'$ are concurrent, then the perpendicular lines from A', B', C' onto BC, CA, AB are concurrent.

11. Let ABC be a triangle and suppose there is a point M such that $MA_1 \perp MA$, $MB_1 \perp MB$, $MC_1 \perp MC$, with $A_1 \in BC$, $B_1 \in CA$, $C_1 \in AB$. Prove that the points A_1, B_1, C_1 are collinear.

12. Let $A_1A_2A_3A_4$ be a tangential quadrilateral (that is, it has an incircle — a circle within the quadrilateral, tangent to all its sides). Prove that $A_1A_2A_3A_4$ is also cyclic if and only if the lines passing through the tangency points of the incircle with opposite sides of the quadrilateral are perpendicular.

13. Let $ABCD$ be a tetrahedron such that $AD \perp BC$ and $AC \perp BD$. Prove that $AB \perp CD$.

14. Let $A_1A_2A_3A_4A_5$ be a pentagon such that the altitudes from A_2, A_3, A_4, A_5 are concurrent. Prove that all five altitudes of the pentagon are concurrent. (By an *altitude* of a pentagon, we mean for each $1 \leq k \leq 5$, the perpendicular line onto A_kA_{k+1}, passing through A_{k+3}, with the convention $A_{k+5} = A_k$).

15. Let $A_1, \dots, A_n$ be points in space, and let $w_1, \dots, w_n$ be real numbers with $w = w_1 + \dots + w_n \neq 0$. One can show (prove it!) that there exists a unique point X in space such that
$$w_1\overrightarrow{XA_1} + \dots + w_n\overrightarrow{XA_n} = \overrightarrow{0}$$

(X is the center of mass of weighted points (A_i, w_i)). Prove Leibniz's theorem in one of the forms:

$$\sum_{i=1}^{n} w_i MA_i^2 = \sum_{i=1}^{n} w_i XA_i^2 + wMX^2$$

or

$$w\sum_{i=1}^{n} w_i MA_i^2 = \sum_{1\le i<j\le n} w_i w_j A_i A_j^2 + w^2 MX^2,$$

where M can be any point in space. Infer that if $w_1, \ldots, w_n$ have positive sum, then

$$\sum_{i=1}^{n} w_i MA_i^2 \ge \sum_{i=1}^{n} w_i XA_i^2,$$

for any point M, with equality if and only if $M = X$.

16. Let $ABCD$ be a tetrahedron for which $K_{ABC} = K_{ABD}$ and $K_{ACD} = K_{BCD}$ hold (where K_{XYX} denotes the area of triangle XYZ). Prove that in this tetrahedron, we have $AC = BD$ and $AD = BC$.

Solutions

1. Let ABC be a right triangle with $m(\angle BAC) = 90°$, and let AD be the altitude from vertex A (with $D \in BC$). We thus want to prove that $AD^2 = BD \cdot DC$ (the length of the altitude from the right angle's vertex is the geometric mean of the lengths of segments determined by the altitude's foot on the hypotenuse). We have

$$\begin{aligned} BD \cdot DC &= \overrightarrow{BD} \cdot \overrightarrow{DC} = (\overrightarrow{AD} - \overrightarrow{AB})(\overrightarrow{AC} - \overrightarrow{AD}) \\ &= \overrightarrow{AD} \cdot \overrightarrow{AC} - \overrightarrow{AD}^2 + \overrightarrow{AB} \cdot \overrightarrow{AD} \\ &= \overrightarrow{AD}^2 + \overrightarrow{AD}(\overrightarrow{AB} - \overrightarrow{AD} + \overrightarrow{AC} - \overrightarrow{AD}) \\ &= AD^2 + \overrightarrow{AD} \cdot (\overrightarrow{DB} + \overrightarrow{DC}) = AD^2. \end{aligned}$$

We used $\overrightarrow{AB} \cdot \overrightarrow{AC} = \overrightarrow{AD} \cdot \overrightarrow{DB} = \overrightarrow{AD} \cdot \overrightarrow{DC} = 0$ (by perpendicularity).

Try to prove, for example, that (with the same notations as above) $AB^2 = BD \cdot BC$ with the help of the scalar product (which is the other part of the altitude to the hypotenuse theorem, that is, the length of one leg of a right triangle is the geometric mean of the length of the hypotenuse and the length of the projection on the hypotenuse of that leg).

2. **Solution I.** We have $2\overrightarrow{DM} = \overrightarrow{DA} + \overrightarrow{DB}$ (because M is the midpoint of AB), and $2\overrightarrow{AN} = \overrightarrow{AB} + \overrightarrow{AC}$ (because N is the midpoint of BC). Consequently,

$$4\overrightarrow{DM} \cdot \overrightarrow{AN} = \overrightarrow{DA} \cdot \overrightarrow{AC} + \overrightarrow{DB} \cdot \overrightarrow{AB} = 0,$$

and the conclusion follows. We used $\overrightarrow{DA} \cdot \overrightarrow{AB} = \overrightarrow{DB} \cdot \overrightarrow{AC} = 0$ (by perpendicularity), and

$$-\overrightarrow{DA} \cdot \overrightarrow{AC} = \overrightarrow{DB} \cdot \overrightarrow{AB} = l^2$$

(where l is the length of the side of the square $ABCD$), by the definition of scalar product.

Solution II. We have

$$\overrightarrow{DM} \cdot \overrightarrow{AN} = (\overrightarrow{DA} + \overrightarrow{AM}) \cdot (\overrightarrow{AB} + \overrightarrow{BN}) = \overrightarrow{DA} \cdot \overrightarrow{BN} + \overrightarrow{AM} \cdot \overrightarrow{AB} = 0,$$

yielding the conclusion. This time we used $\overrightarrow{DA} \cdot \overrightarrow{AB} = \overrightarrow{AM} \cdot \overrightarrow{BN} = 0$ (by perpendicularity), and

$$-\overrightarrow{DA} \cdot \overrightarrow{BN} = \overrightarrow{AM} \cdot \overrightarrow{AB} = \frac{l^2}{2}$$

by the definition of the scalar product.

3. We have $2\overrightarrow{AD} = \overrightarrow{AB} + \overrightarrow{AC}$ (D being the midpoint of BC), and

$$3\overrightarrow{BE} = \overrightarrow{AC} - 3\overrightarrow{AB}$$

(equivalent to $3\overrightarrow{AE} = \overrightarrow{AC}$). Thus

$$6\overrightarrow{AD} \cdot \overrightarrow{BE} = (\overrightarrow{AB} + \overrightarrow{AC}) \cdot (\overrightarrow{AC} - 3\overrightarrow{AB}) = AC^2 - 3AB^2 = 0,$$

because $\overrightarrow{AB} \cdot \overrightarrow{AC} = 0$ and $AC/AB = \cot 30^\circ = \sqrt{3}$.

Try to solve the problem without using the scalar product.
(Hint: triangle ABD is equilateral, and BE is the bisector of $\angle ABD$.)

4. We have $2\overrightarrow{CM} = \overrightarrow{CA} + \overrightarrow{CD} = 2\overrightarrow{CD} - \overrightarrow{AD}$ and

$$2\overrightarrow{AN} = \overrightarrow{AB} + \overrightarrow{AD} = 2\overrightarrow{AD} + \overrightarrow{DB},$$

hence

$$\begin{aligned} 4\overrightarrow{CM} \cdot \overrightarrow{AN} &= (2\overrightarrow{CD} - \overrightarrow{AD}) \cdot (2\overrightarrow{AD} + \overrightarrow{DB}) \\ &= 2(\overrightarrow{CD} \cdot \overrightarrow{DB} - \overrightarrow{AD} \cdot \overrightarrow{AD}) \\ &= 2(CD \cdot BD - AD^2) = 0 \end{aligned}$$

because $\overrightarrow{CD} \cdot \overrightarrow{AD} = \overrightarrow{AD} \cdot \overrightarrow{DB} = 0$ and $CD \cdot BD = AD^2$ due to the altitude to the hypotenuse theorem.

Again, try to solve the problem by classic Euclidean geometry. (Hint: what special point is M for triangle NAC?)

5. We have $2\overrightarrow{MN} = \overrightarrow{AD} + \overrightarrow{BC}$ and $2\overrightarrow{PQ} = \overrightarrow{AD} - \overrightarrow{BC}$ (see the proof of Euler's relation), therefore

$$4\overrightarrow{MN} \cdot \overrightarrow{PQ} = AD^2 - BC^2.$$

Clearly, the conclusion follows.

Try to solve this one by synthetic methods too (no hint this time!). Note that such methods can be considered simpler than the use of the scalar product for all of the above problems. However, we included them here because (at least) for the reader who is less familiar with the scalar product, these are very good exercises for practice.

6. With the notations $\overrightarrow{AB} = \vec{b}$, $\overrightarrow{AC} = \vec{c}$, $\overrightarrow{AD} = \vec{d}$, we have

$$\begin{aligned}
&\overrightarrow{CD} = \vec{d} - \vec{c},\ \overrightarrow{BC} = \vec{c} - \vec{b},\\
&\overrightarrow{KM} = \overrightarrow{AM} - \overrightarrow{AK} = \frac{1}{2}(\vec{d} + \vec{c} - \vec{b}),\\
&\overrightarrow{LN} = \overrightarrow{AN} - \overrightarrow{AL} = \frac{1}{2}(\vec{d} - \vec{b} - \vec{c}),
\end{aligned}$$

so

$$\begin{aligned}
(\overrightarrow{AB}^2 + \overrightarrow{CD}^2) - (\overrightarrow{AD}^2 + \overrightarrow{BC}^2) &= \left[\vec{b}^2 + (\vec{d} - \vec{c})^2\right] - \left[\vec{d}^2 + (\vec{c} - \vec{b})^2\right]\\
&= 2\vec{c}(\vec{b} - \vec{d}) = 2\overrightarrow{AC} \cdot \overrightarrow{DB}.
\end{aligned}$$

(And we have an alternative calculation of the scalar product $\overrightarrow{AC} \cdot \overrightarrow{DB}$ in terms of lengths of some line segments.) Yet

$$\begin{aligned}
4(\overrightarrow{LN}^2 - \overrightarrow{KM}^2) &= (\vec{d} - \vec{b} - \vec{c})^2 - (\vec{d} + \vec{c} - \vec{b})^2\\
&= 4\vec{c}(\vec{b} - \vec{d}) = 4\overrightarrow{AC} \cdot \overrightarrow{DB}.
\end{aligned}$$

As an application, in each convex quadrilateral, the following assertions are equivalent:

i) the diagonals are perpendicular;

ii) the segments joining the midpoints of opposite sides are congruent;

iii) the sum of the squares of the lengths of two opposite sides equals the sum of the squares of the lengths of the remaining two sides.

7. We prove that $\overrightarrow{AM} \cdot \overrightarrow{B'C'} = 0$, where M is the midpoint of BC. We have

$$\begin{aligned}
\overrightarrow{AM} \cdot \overrightarrow{B'C'} &= \frac{1}{2}(\overrightarrow{AB} + \overrightarrow{AC})(\overrightarrow{HC'} - \overrightarrow{HB'}) \\
&= \frac{1}{2}(\overrightarrow{AB} \cdot \overrightarrow{HC'} - \overrightarrow{AB} \cdot \overrightarrow{HB'} + \overrightarrow{AC} \cdot \overrightarrow{HC'} - \overrightarrow{AC} \cdot \overrightarrow{HB'}) \\
&= \frac{1}{2}(\overrightarrow{AC} \cdot \overrightarrow{HC'} - \overrightarrow{AB} \cdot \overrightarrow{HB'}).
\end{aligned}$$

But $\angle(AC, HC') = \angle(AB, HB') = \frac{\pi}{2} - \angle A$, so

$$\overrightarrow{AM} \cdot \overrightarrow{B'C'} = \frac{1}{2}(bc\sin A - bc\sin A) = 0.$$

8. We have $\overrightarrow{RN} = \frac{1}{2}(\overrightarrow{FB} + \overrightarrow{EC})$ and analogously, so $\overrightarrow{RN} + \overrightarrow{MQ} + \overrightarrow{PS} = \overrightarrow{0}$. Therefore $\overrightarrow{NR} = \overrightarrow{MQ} + \overrightarrow{PS}$ and

$$NR^2 = MQ^2 + PS^2 + 2\overrightarrow{MQ} \cdot \overrightarrow{PS}.$$

Now the condition $NR^2 = MQ^2 + PS^2$ is equivalent to $\overrightarrow{MQ} \cdot \overrightarrow{PS} = 0$, that is $MQ \perp PS$.

9. We have

$$\begin{aligned}
\overrightarrow{OE} = \frac{1}{3}\left(\overrightarrow{OA} + \overrightarrow{OC} + \overrightarrow{OD}\right) &= \frac{1}{3}\left(\overrightarrow{OA} + \overrightarrow{OC} + \frac{1}{2}(\overrightarrow{OA} + \overrightarrow{OB})\right) \\
&= \frac{1}{6}\left(3\overrightarrow{OA} + 2\overrightarrow{OC} + \overrightarrow{OB}\right)
\end{aligned}$$

and

$$\overrightarrow{CD} = \overrightarrow{OD} - \overrightarrow{OC} = \frac{1}{2}\left(\overrightarrow{OA} + \overrightarrow{OB}\right) - \overrightarrow{OC} = \frac{1}{2}\left(\overrightarrow{OA} + \overrightarrow{OB} - 2\overrightarrow{OC}\right)$$

so

$$\overrightarrow{OE} \cdot \overrightarrow{CD} = \frac{1}{12}\left(4\overrightarrow{OA} \cdot \overrightarrow{OB} - 4\overrightarrow{OA} \cdot \overrightarrow{OC}\right) = \frac{1}{3}\overrightarrow{OA} \cdot \left(\overrightarrow{OB} - \overrightarrow{OC}\right).$$

We proved that $\overrightarrow{OE} \cdot \overrightarrow{CD} = \frac{1}{3}\overrightarrow{OA} \cdot \overrightarrow{CB}$. If $OE \perp CD$, then

$$\overrightarrow{OE} \cdot \overrightarrow{CD} = \overrightarrow{0} \Rightarrow \overrightarrow{OA} \cdot \overrightarrow{CB} = \overrightarrow{0},$$

which is equivalent to $OA \perp BC$ and finally, $AB = AC$.

10. Let O be the intersection point of the perpendiculars through A, B, C. Let O' be the intersection point of the perpendiculars through A', B', on BC and CA, respectively. Denote $\overrightarrow{OA} = \vec{a}$, $\overrightarrow{OB} = \vec{b}$, $\overrightarrow{OC} = \vec{c}$, $\overrightarrow{O'A'} = \overrightarrow{a'}$, $\overrightarrow{O'B'} = \overrightarrow{b'}$, $\overrightarrow{O'C'} = \overrightarrow{c'}$. We have
$$\overrightarrow{a'}(\vec{c} - \vec{b}) = \overrightarrow{b'}(\vec{a} - \vec{c}) = 0,$$
so $\vec{a} \cdot \overrightarrow{b'} = \vec{b} \cdot \overrightarrow{a'} = \vec{b} \cdot \overrightarrow{c'} = \vec{c} \cdot \overrightarrow{a'} = \vec{c} \cdot \overrightarrow{b'}$. It follows that $\overrightarrow{c'}(\vec{b} - \vec{a}) = 0$, thus $O'C' \perp AB$.

11. With the notations $\overrightarrow{MA} = \vec{a}$, $\overrightarrow{MB} = \vec{b}$, $\overrightarrow{MC} = \vec{c}$ and
$$\frac{\overrightarrow{AC_1}}{\overrightarrow{C_1B}} = \frac{p_1}{q_1},\ \frac{\overrightarrow{BA_1}}{\overrightarrow{A_1C}} = \frac{p_2}{q_2},\ \frac{\overrightarrow{CB_1}}{\overrightarrow{B_1A}} = \frac{p_3}{q_3},$$
(thus we considered signed ratios) we have
$$\overrightarrow{MC_1} = \frac{p_1\vec{b} + q_1\vec{a}}{p_1 + q_1},\ \overrightarrow{MA_1} = \frac{p_2\vec{c} + q_2\vec{b}}{p_2 + q_2},\ \overrightarrow{MB_1} = \frac{p_3\vec{a} + q_3\vec{c}}{p_3 + q_3}.$$
By multiplying with $\vec{c}$, $\vec{a}$, respectively $\vec{b}$, we obtain
$$\begin{aligned} 0 = \vec{c} \cdot \overrightarrow{MC_1} &\Rightarrow p_1\vec{b} \cdot \vec{c} = -q_1\vec{a} \cdot \vec{c} \\ 0 = \vec{a} \cdot \overrightarrow{MA_1} &\Rightarrow p_2\vec{a} \cdot \vec{c} = -q_2\vec{a} \cdot \vec{b} \\ 0 = \vec{b} \cdot \overrightarrow{MB_1} &\Rightarrow p_3\vec{a} \cdot \vec{b} = -q_3\vec{b} \cdot \vec{c}. \end{aligned}$$
Finally,
$$\frac{p_1}{q_1} \cdot \frac{p_2}{q_2} \cdot \frac{p_3}{q_3} = -\frac{\vec{a} \cdot \vec{c}}{\vec{b} \cdot \vec{c}} \cdot \frac{\vec{a} \cdot \vec{b}}{\vec{a} \cdot \vec{c}} \cdot \frac{\vec{b} \cdot \vec{c}}{\vec{a} \cdot \vec{b}} = -1,$$
thus A_1, B_1, C_1 are collinear.

12. Let O be the incenter of the quadrilateral and denote $\vec{r}_i = \overrightarrow{OM_i}$, where M_i are the tangency points of the inscribed circle with side A_iA_{i+1} $(A_5 = A_1)$.

We have
$$\vec{r}_1^{\,2} = \vec{r}_2^{\,2} = \vec{r}_3^{\,2} = \vec{r}_4^{\,2}$$
and
$$\vec{r}_1 \cdot \vec{r}_2 + \vec{r}_3 \cdot \vec{r}_4 = \vec{r}_3 \cdot \vec{r}_2 + \vec{r}_1 \cdot \vec{r}_4 = 0$$
by the definition of scalar product and because $A_1A_2A_3A_4$ is also cyclic (hence its opposite angles sum to 180°). It follows
$$\overrightarrow{M_1M_3} \cdot \overrightarrow{M_2M_4} = (\vec{r}_3 - \vec{r}_1)(\vec{r}_4 - \vec{r}_2) = 0,$$

so $M_1M_3 \perp M_2M_4$.

Conversely, if $M_1M_3 \perp M_2M_4$, then

$$\vec{r}_1^{\,2} = \vec{r}_2^{\,2} = \vec{r}_3^{\,2} = \vec{r}_4^{\,2}$$

and

$$(\vec{r}_3 - \vec{r}_1)(\vec{r}_4 - \vec{r}_2) = 0,$$

hence

$$\vec{r}_1 \cdot \vec{r}_2 + \vec{r}_3 \cdot \vec{r}_4 = \vec{r}_3 \cdot \vec{r}_2 + \vec{r}_1 \cdot \vec{r}_4.$$

Because the lengths of $\vec{r}_1$, $\vec{r}_2$, $\vec{r}_3$, and $\vec{r}_4$ are equal, the last equation becomes

$$\cos(180^\circ - A_1) + \cos(180^\circ - A_3) = \cos(180^\circ - A_2) + \cos(180^\circ - A_4)$$

or

$$\cos A_1 + \cos A_3 = \cos A_2 + \cos A_4,$$

that is,

$$2\cos\frac{A_1 + A_3}{2}\cos\frac{A_1 - A_3}{2} = 2\cos\frac{A_2 + A_4}{2}\cos\frac{A_2 - A_4}{2},$$

where A_1, A_2, A_3, A_4 also denote the measures of quadrilateral's angles with vertices in the respective points. We have

$$A_1 + A_2 + A_3 + A_4 = 360^\circ,$$

thus

$$\cos((A_1 + A_3)/2) = -\cos((A_2 + A_4)/2).$$

If these cosines are not equal to zero we can simplify them in the above equation to get

$$\cos((A_1 - A_3)/2) = -\cos((A_2 - A_4)/2),$$

but this equality leads to a contradiction (check that!). Therefore

$$\cos((A_1 + A_3)/2) = -\cos((A_2 + A_4)/2) = 0,$$

that is

$$A_1 + A_3 = A_2 + A_4 = 180^\circ$$

and $A_1A_2A_3A_4$ is cyclic, as we intended to prove.

13. We have

$$\overrightarrow{DA}\cdot\overrightarrow{BC}+\overrightarrow{DB}\cdot\overrightarrow{CA}+\overrightarrow{DC}\cdot\overrightarrow{AB}$$
$$=\overrightarrow{DA}\cdot(\overrightarrow{DC}-\overrightarrow{DB})+\overrightarrow{DB}\cdot(\overrightarrow{DA}-\overrightarrow{DC})+\overrightarrow{DC}\cdot(\overrightarrow{DB}-\overrightarrow{DA})=0.$$

Thus, if we have $AD\perp BC$ and $AC\perp BD$, the first and the second scalar product from the left hand side of this equality being zero, the third must be zero, too — that is, AB and CD are also perpendicular.

Again, it is not necessary for A, B, C, D to be the vertices of a tetrahedron — they can be any points in space. For instance, if they are in the same plane, this is a proof of the concurrence of the altitudes of a triangle. Prove also that if $AD\perp BC$ and $AC\perp BD$ (and thus, $AB\perp CD$, too) we have $AB^2+CD^2=AC^2+BD^2=AD^2+BC^2$. (Remember the expression of a scalar product like $\overrightarrow{AB}\cdot\overrightarrow{CD}$ in terms of lengths of some line segments!)

14. Basically it is the same idea as in the previous problem. Let H be the common point of the altitudes passing through A_2, A_3, A_4, A_5. Because we have

$$\overrightarrow{HA_1}\cdot(\overrightarrow{HA_3}-\overrightarrow{HA_4})+\overrightarrow{HA_2}\cdot(\overrightarrow{HA_4}-\overrightarrow{HA_5})+\overrightarrow{HA_3}\cdot(\overrightarrow{HA_5}-\overrightarrow{HA_1})$$
$$+\overrightarrow{HA_4}\cdot(\overrightarrow{HA_1}-\overrightarrow{HA_2})+\overrightarrow{HA_5}\cdot(\overrightarrow{HA_2}-\overrightarrow{HA_3})=0,$$

that is,

$$\overrightarrow{HA_1}\cdot\overrightarrow{A_4A_3}+\overrightarrow{HA_2}\cdot\overrightarrow{A_5A_4}+\overrightarrow{HA_3}\cdot\overrightarrow{A_1A_5}+\overrightarrow{HA_4}\cdot\overrightarrow{A_2A_1}+\overrightarrow{HA_5}\cdot\overrightarrow{A_3A_2}=0$$

and all scalar products in this equality starting with the second are zero, the first scalar product has to be zero, too, meaning that $HA_1\perp A_3A_4$, that is, the altitude from A_1 passes through H, too.

15. If we square $\overrightarrow{MA_i}=\overrightarrow{MX}+\overrightarrow{XA_i}$ we get

$$MA_i^2=XA_i^2+MX^2+2\overrightarrow{MX}\cdot\overrightarrow{XA_i}.$$

Now we multiply this by w_i, add for i from 1 to n, and thus obtain

$$\sum_{i=1}^{n}w_iMA_i^2=\left(\sum_{i=1}^{n}w_iXA_i^2\right)+wMX^2+2\overrightarrow{MX}\cdot\left(\sum_{i=1}^{n}w_i\overrightarrow{XA_i}\right),$$

that is, the required (first) equality, because $\sum_{i=1}^{n}w_i\overrightarrow{XA_i}=\overrightarrow{0}$.

For the second equality, start by squaring $\sum_{i=1}^{n} w_i\overrightarrow{XA_i} = \overrightarrow{0}$:

$$\sum_{i=1}^{n} w_i^2 XA_i^2 + 2 \cdot \sum_{1\le i<j\le n} w_i w_j \overrightarrow{XA_i} \cdot \overrightarrow{XA_j} = 0.$$

But $2\overrightarrow{XA_i} \cdot \overrightarrow{XA_j} = XA_i^2 + XA_j^2 - A_iA_j^2$, hence the above equality becomes

$$\sum_{i=1}^{n} w_i^2 XA_i^2 + \sum_{1\le i<j\le n} w_i w_j (XA_i^2 + XA_j^2 - A_iA_j^2) = 0.$$

Since

$$\sum_{i=1}^{n} w_i^2 XA_i^2 + \sum_{1\le i<j\le n} w_i w_j (XA_i^2 + XA_j^2) = \left(\sum_{i=1}^{n} w_i\right)\left(\sum_{i=1}^{n} w_i XA_i^2\right),$$

it follows that

$$\sum_{i=1}^{n} w_i XA_i^2 = \frac{1}{w} \sum_{1\le i<j\le n} w_i w_j A_iA_j^2,$$

and, by replacing this in the right hand side of the first form of Leibniz's theorem, we get the second one.

The inequality is an immediate consequence of Leibniz's theorem (in the first form), as $wMX^2 \ge 0$. Clearly, we have equality if and only if $MX = 0$, that is, if and only if $M = X$.

Note also that from the second form of Leibniz's theorem, the inequality

$$w \sum_{i=1}^{n} w_i MA_i^2 \ge \sum_{1\le i<j\le n} w_i w_j A_iA_j^2,$$

can be deduced in a similar manner, again with equality if and only if $M = X$. This time we don't need the assumption $w > 0$, because we use $w^2MX^2 \ge 0$.

Remarks. 1) For $w_1 = \cdots = w_n = 1$, the point X is the centroid G of the points $A_1, \ldots, A_n$, that is, G is defined by the vector equation

$$\overrightarrow{GA_1} + \cdots + \overrightarrow{GA_n} = \overrightarrow{0},$$

or

$$\overrightarrow{MA_1} + \cdots + \overrightarrow{MA_n} = n\overrightarrow{MG}$$

for every point M. Leibniz's formula in this case reads either

$$\sum_{i=1}^{n} MA_i^2 = \sum_{i=1}^{n} GA_i^2 + nMG^2$$

or

$$n\sum_{i=1}^{n} MA_i^2 = \sum_{1\le i<j\le n} A_iA_j^2 + n^2MG^2,$$

for an arbitrary point M, and we have

$$\sum_{i=1}^{n} GA_i^2 = \frac{1}{n}\sum_{1\le i<j\le n} A_iA_j^2.$$

2) The centroid G of a triangle ABC is the (well-known) intersection of its medians, and it verifies

$$MA^2 + MB^2 + MC^2 = GA^2 + GB^2 + GC^2 + 3MG^2$$

(the most widely known form of Leibniz's theorem), or, equivalently,

$$3(MA^2 + MB^2 + MC^2) = a^2 + b^2 + c^2 + 9MG^2$$

(with the usual notations $a = BC$, $b = AC$, $c = AB$). For $M = O$ (the circumcenter of triangle ABC), we obtain

$$OG^2 = R^2 - \frac{1}{9}(a^2 + b^2 + c^2)$$

($R = OA = OB = OC$ being the circumradius of ABC), and the inequality $a^2 + b^2 + c^2 \le 9R^2$, with equality only in the case of an equilateral triangle.

3) Check that the centroid G of a tetrahedron $ABCD$ (or, in general, of an arbitrary system of four equally weighted points A, B, C, and D in space, possibly the vertices of a quadrilateral) is the intersection of its four medians and three bimedians. A median is the line through one vertex and the centroid of the remaining three (for instance, one median passes through A and the centroid of triangle BCD), and a bimedian joins the midpoints of two opposite edges (like AB and CD). Leibniz's equation in this case is

$$MA^2 + MB^2 + MC^2 + MD^2 = GA^2 + GB^2 + GC^2 + GD^2 + 4MG^2,$$

or one can replace here

$$GA^2+GB^2+GC^2+GD^2 = \frac{1}{4}(AB^2+AC^2+AD^2+BC^2+BD^2+CD^2).$$

4) As a final example (but there still are many — the reader can enjoy finding them), consider again a triangle ABC with lengths of the sides $a = BC$, $b = AC$, and $c = AB$. It is well-known that the incenter I of triangle ABC is the center of mass of weighted points (A, a), (B, b), and (C, c), that is

$$a\overrightarrow{IA} + b\overrightarrow{IB} + c\overrightarrow{IC} = \overrightarrow{0},$$

or, equivalently,

$$a\overrightarrow{MA} + b\overrightarrow{MB} + c\overrightarrow{MC} = (a + b + c)\overrightarrow{MI},$$

for any point M. Leibniz's relation states in this case that

$$aMA^2 + bMB^2 + cMC^2 = aIA^2 + bIB^2 + cIC^2 + (a + b + c)MI^2,$$

or that

$$(a+b+c)(aMA^2+bMB^2+cMC^2) = abc^2+acb^2+bca^2+(a+b+c)^2MI^2$$

$$\Leftrightarrow aMA^2 + bMB^2 + cMC^2 = abc + (a + b + c)MI^2$$

for every point M. Specializing for $M = O$ (the circumcenter) we obtain

$$(a + b + c)R^2 = abc + (a + b + c)OI^2,$$

or

$$OI^2 = R^2 - \frac{abc}{a + b + c}.$$

Now, by the well-known equation $abc = 4Rrs$ (with r the inradius and $s = (a + b + c)/2$ the semiperimeter of triangle ABC), this yields another celebrated formula of Euler, namely the one that gives the distance between the circumcenter and the incenter of a triangle:

$$OI^2 = R^2 - 2Rr.$$

Euler's inequality $R \geq 2r$ (with equality if and only if the triangle is equilateral) is an obvious consequence of this formula — and note that it is related to the inequality from the result of our problem.

16. This is not exactly related to the scalar product, but it uses the above proved formula of Euler for four arbitrary points in space. Also, we put this beautiful result here because we think that the (quasi)algebraic proof that follows (based on Heron's formula for the area of a triangle) is very natural and nice, and it is also very little known; actually, it is not known at all — at least we never met it before in any other source. Actually, the more symmetric result stating that a tetrahedron with

equal areas of faces is equifacial (that is, it has every edge congruent to its opposite edge) is the one that reveals an exquisite beauty. The reader understands immediately that this result is a consequence of the problem discussed below.

We set $a = BC$, $b = AC$, $c = AB$, $x = AD$, $y = BD$, $z = CD$. By Heron's mentioned formula (with $s = (a+b+c)/2$),

$$\begin{aligned} K_{ABC} &= \sqrt{s(s-a)(s-b)(s-c)} \\ &= \frac{1}{4}\sqrt{2a^2b^2 + 2a^2c^2 + 2b^2c^2 - a^4 - b^4 - c^4} \end{aligned}$$

and analogous formulas for the other areas hold, thus the hypothesis can be expressed in the equations

$$2a^2b^2 + 2a^2c^2 + 2b^2c^2 - a^4 - b^4 - c^4 = 2c^2x^2 + 2c^2y^2 + 2x^2y^2 - c^4 - x^4 - y^4$$

and

$$2b^2x^2 + 2b^2z^2 + 2x^2z^2 - b^4 - x^4 - z^4 = 2a^2y^2 + 2a^2z^2 + 2y^2z^2 - a^4 - y^4 - z^4.$$

We can rewrite the first equality as

$$(x^2 - y^2)^2 - (a^2 - b^2)^2 = 2c^2(x^2 + y^2 - a^2 - b^2),$$

or

$$(x^2 - y^2 - a^2 + b^2)(x^2 - y^2 + a^2 - b^2) = 2c^2(x^2 + y^2 - a^2 - b^2),$$

and, similarly, the second equality becomes

$$(x^2 + y^2 - a^2 - b^2)(x^2 - y^2 + a^2 - b^2) = 2z^2(x^2 - y^2 - a^2 + b^2).$$

By multiplying side by side the above two equations and rearranging a little, we obtain

$$(x^2 - y^2 - a^2 + b^2)(x^2 + y^2 - a^2 - b^2)((x^2 - y^2 + a^2 - b^2)^2 - 4c^2z^2) = 0.$$

Now we see that each of the equalities

$$x^2 + y^2 - a^2 - b^2 = 0 \quad \text{and} \quad x^2 - y^2 - a^2 + b^2 = 0$$

implies the other one, and the two of them lead (by addition and subtraction) to $x = a$ and $y = b$, which is exactly what we intended to prove. So it only remains to see what happens if the third factor above is zero, otherwise the proof is done. We show further that actually the third factor is never zero. In order to do that, let M, N, P, Q be the midpoints of edges AC, BC, AD, and BD, respectively. We have, according to Euler's result,

$$4NP^2 = b^2 + c^2 + y^2 + z^2 - a^2 - x^2$$

and

$$4MQ^2 = a^2 + c^2 + x^2 + z^2 - b^2 - y^2.$$

The triangle inequality (in triangle NPQ, for example) says that

$$NP < PQ + QN, \quad \text{that is,} \quad NP < (c+z)/2.$$

Consequently, we have

$$(c+z)^2 > 4NP^2 = b^2+c^2+y^2+z^2-a^2-x^2 \Rightarrow 2cz > -(x^2-y^2+a^2-b^2).$$

Applying the triangle inequality again (in triangle MPQ) assures that

$$MQ < MP + PQ = (c+z)/2,$$

yielding

$$(c+z)^2 > 4MQ^2 = a^2+c^2+x^2+z^2-b^2-y^2 \Rightarrow 2cz > x^2-y^2+a^2-b^2.$$

Thus we have $2cz > |x^2-y^2+a^2-b^2|$, hence $4c^2z^2 > (x^2-y^2+a^2-b^2)^2$ meaning that (as claimed) the third factor is never zero. The proof is now complete.

Chapter 10

Equilateral Triangles in the Complex Plane

A large number of problems involving equilateral triangles can be easily solved using the geometric interpretation of complex numbers.

Each complex number $z = x + iy$ can be identified with the point $M(x, y)$ from the xy-plane. Let $r = OM$ and let α be the angle between OM and the positive direction of the x-axis. We have

$$x = r\cos\alpha, \quad y = r\sin\alpha,$$

thus

$$x + iy = r(\cos\alpha + i\sin\alpha)$$

will be the trigonometric form of a complex number. Conversely, $r = \sqrt{x^2 + y^2}$ is the absolute value of $z = x + iy$, denoted by $|z|$, and the angle $\alpha \in [0, 2\pi)$ given by

$$\cos\alpha = \frac{x}{\sqrt{x^2 + y^2}}\quad , \quad \sin\alpha = \frac{y}{\sqrt{x^2 + y^2}},$$

is called the argument of $z = x + iy$. From the identity

$$(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \cos(\alpha + \beta) + i\sin(\alpha + \beta)$$

one obtains the formulas

$$\arg(z_1 z_2) = \arg z_1 + \arg z_2 \pmod{2\pi}$$

and

$$\arg\left(\frac{z_1}{z_2}\right) = \arg z_1 - \arg z_2 \pmod{2\pi}.$$

In the Cartesian plane, the distance between $A(a_1, a_2)$ and $B(b_1, b_2)$ is

$$AB = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}.$$

If we consider also the corresponding complex numbers

$$z_A = a_1 + ia_2 \quad , \quad z_B = b_1 + ib_2$$

we see that

$$|z_A - z_B| = |(a_1 - b_1) + i(a_2 - b_2)| = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}.$$

Thus we have the formula

$$AB = |z_A - z_B|\,.$$

In what follows we will denote by z_A, $z_B, z_C, \ldots, z_M, \ldots$ (or simply by $a, b, c, \ldots, m, \ldots$) the complex numbers corresponding to the points A, B, $C, \ldots$, $M, \ldots$ from the xy-plane.

Let $A(a_1, a_2)$ and $B(b_1, b_2)$ be two points in the xy-plane. We have $\angle AOx = \arg z_A$, $\angle BOx = \arg z_B$, so

$$\angle AOB = \angle AOx - \angle BOx = \arg z_A - \arg z_B = \arg\left(\frac{z_A}{z_B}\right).$$

Further, we want to give a formula for the angle $\angle ACB$ in complex terms, where C is the point $C(c_1, c_2)$.

Let A', B' be such that the quadrilaterals $OA'AC$ and $OB'BC$ are parallelograms. Obviously,

$$z_{A'} = z_A - z_C \quad , \quad z_{B'} = z_B - z_C.$$

Then

$$\angle ACB = \angle A'OB' = \arg\frac{z_{A'}}{z_{B'}} = \arg\frac{z_A - z_C}{z_B - z_C}.$$

Now, we are in a position to give a necessary and sufficient condition for three numbers a, b, c to be the images of the vertices of an equilateral triangle. To this end, we will use the following characterization: the triangle $A(a)$, $B(b)$, $C(c)$ is equilateral if and only if

$$\angle BAC = \frac{\pi}{3} \quad \text{and} \quad BA = AC.$$

We have

$$\angle BAC = \frac{\pi}{3} \Leftrightarrow \arg\frac{b-a}{c-a} = \frac{\pi}{3} \tag{1}$$

and

$$BA = AC \Leftrightarrow |a - b| = |a - c| \Leftrightarrow \left|\frac{b-a}{c-a}\right| = 1. \tag{2}$$

Further, the relations (1) and (2) are equivalent to

$$\frac{b-a}{c-a} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}.$$

With $\lambda = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$ we have $\lambda^3 = -1$ and $\lambda^2 - \lambda + 1 = 0$. Thus

$$\begin{aligned}\frac{b-a}{c-a} = \lambda &\Leftrightarrow a(\lambda - 1) + b - c\lambda = 0\\ &\Leftrightarrow a\lambda^2 + b - c\lambda = 0\end{aligned}$$

and by multiplying by λ^2, we deduce that

$$a\lambda^4 + b\lambda^2 + c = 0.$$

If we denote $\omega = \lambda^2$, $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$, we deduce that

$$a\omega^2 + b\omega + c = 0.$$

If the triangle ABC has inverse orientation, we have

$$a\omega^2 + c\omega + b = 0.$$

Conversely, if $a\omega^2 + b\omega + c = 0$, then $a, b, c \in \mathbb{C}$ are the images of the vertices of an equilateral triangle. Indeed,

$$\begin{aligned}\frac{b-a}{c-a} &= \frac{b-a}{-(a\omega^2 + b\omega) - a} = \frac{b-a}{-a(\omega^2+1) - b\omega}\\ &= \frac{b-a}{a\omega - b\omega} = \frac{b-a}{\omega(a-b)} = -\frac{1}{\omega}\\ &= -\omega^2 = -\lambda^4 = \lambda.\end{aligned}$$

Now, from $\frac{b-a}{c-a} = \lambda$, it follows

$$\left|\frac{b-a}{c-a}\right| = 1 \Rightarrow |b-a| = |c-a| \Rightarrow AB = AC$$

and

$$\angle BAC = \arg\frac{b-a}{c-a} = \arg\lambda = \frac{\pi}{3},$$

so the triangle ABC is equilateral.

We proved that $a, b, c \in \mathbb{C}$ are the vertices of an equilateral triangle if and only if

$$a\omega^2 + b\omega + c = 0 \quad \text{or} \quad a\omega^2 + c\omega + b = 0, \tag{3}$$

where $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$. Note that $\omega^3 = 1$ and $\omega^2 + \omega + 1 = 0$.

As a direct consequence, if $a, b \in \mathbb{C}$ are given, then we can easily find the third vertex $c \in \mathbb{C}$ of the equilateral triangle; it is

$$c = -a\omega^2 - b\omega \quad \text{or} \quad c = -a\omega - b\omega^2,$$

according to the orientation.

Problem. Let $a, b, c \in \mathbb{C}$ be such that

$$a^2 + b^2 + c^2 = ab + bc + ca. \tag{4}$$

Prove that a, b, c are the vertices of an equilateral triangle (eventually $a = b = c$).

Solution I. If a, b, c are vertices of an equilateral triangle, then

$$c = -a\omega^2 - b\omega \quad \text{or} \quad c = -a\omega - b\omega^2.$$

With these values, (4) is obviously satisfied.
Conversely, if (4) holds true, we infer

$$c^2 - (a + b)c + a^2 + b^2 - ab = 0, \tag{5}$$

which is a quadratic equation in c. For given $a, b \in \mathbb{C}$, there exist at most two values of c satisfying (5). But we have seen that

$$c = -a\omega^2 - b\omega \quad \text{and} \quad c = -a\omega - b\omega^2 \tag{6}$$

satisfy (5). In conclusion, (5) implies (6) and from (3), a, b, c are the vertices of an equilateral triangle.

Solution II. The given relation is equivalent to

$$(a - b)^2 + (b - c)^2 + (c - a)^2 = 0.$$

With the notations $x = b - a$, $y = c - a$, we derive

$$x^2 + y^2 + (x - y)^2 = 0 \Rightarrow x^2 - xy + y^2 = 0.$$

If $y = 0$, then $x = 0$ and so $a = b = c$. If $y \neq 0$, then

$$\left(\frac{x}{y}\right)^2 - \frac{x}{y} + 1 = 0.$$

It follows that

$$\frac{x}{y} = \lambda \Leftrightarrow \frac{b - a}{c - a} = \lambda,$$

so the conclusion is true. The other case is analogous.

Solution III. We have seen that the given relation is equivalent to (3). So the idea is to compute the product

$$\left(a\omega^2+b\omega+c\right)\left(a\omega^2+c\omega+b\right).$$

If you use the properties of ω, you will have a nice surprise:

$$\left(a\omega^2+b\omega+c\right)\left(a\omega^2+c\omega+b\right)=a^2+b^2+c^2-ab-bc-ca$$

and now, the conclusion follows.

Problem. Let A, B, C be three collinear points, B between A and C. On the same semiplane determined by AC, we consider the equilateral triangles ABM, BCN. Let D and E be the respective midpoints of AN and MC. Prove that the triangle BDE is equilateral. Moreover, the centroid of the triangle BDE is the midpoint of the segment determined by the centroids of the triangles AMB and BNC.

Solution. Let $A(0)$, $B(b)$, $C(c)$ be with $b, c \in \mathbb{R}$, $0<b<c$. This fact is possible if we consider the complex plane with origin A and with $\overrightarrow{AC}$ as positive real axis. Using (3), we obtain

$$m+\omega\cdot 0+\omega^2 b=0, \quad n+\omega b+\omega^2 c=0,$$

so

$$m=-\omega^2 b, \quad n=-\omega b-\omega^2 c.$$

Further,

$$d=\frac{a+n}{2}=\frac{-\omega b-\omega^2 c}{2}$$

and

$$e=\frac{m+c}{2}=\frac{-\omega^2 b+c}{2}.$$

Now,

$$b+\omega e+\omega^2 d=b+\omega\cdot\frac{-\omega^2 b+c}{2}+\omega^2\cdot\frac{-\omega b-\omega^2 c}{2}=0,$$

so the triangle BDE is equilateral. Finally, we have to verify that

$$\frac{b+d+e}{3}=\frac{1}{2}\left(\frac{a+m+b}{3}+\frac{b+c+n}{3}\right).$$

Before leaving the reader to solve some problems for practice, we discuss two more geometry problems that can be easily solved using these methods.

Problem. Let AOB, COD, and EOF be equilateral triangles having the same orientation. Prove that the midpoints of BC, DE, and FA are the vertices of an equilateral triangle.

Solution. Let O be the origin of the complex plane and let $A(a)$, $C(c)$, $E(e)$. Then $B(a\lambda)$, $D(c\lambda)$, $F(e\lambda)$, where $\lambda = \cos(\pi/3) + i\sin(\pi/3)$, hence $\lambda^3 = -1$ and $\lambda^4 = -\lambda$. Letting M, N, P denote the respective midpoints of BC, DE, FA, we have:

$$M\left(\frac{a\lambda + c}{2}\right), \quad N\left(\frac{c\lambda + e}{2}\right), \quad P\left(\frac{e\lambda + a}{2}\right).$$

Now, with $\omega = \lambda^2$, we have

$$\frac{a\lambda + c}{2} + \frac{c\lambda + e}{2} \cdot \omega + \frac{e\lambda + a}{2} \cdot \omega^2 = \frac{a\lambda + c}{2} + \frac{c\lambda + e}{2} \cdot \lambda^2 + \frac{e\lambda + a}{2} \cdot \lambda^4$$

$$= \left(\frac{a\lambda + c}{2} + \frac{-c + e\lambda^2}{2} + \frac{-e\lambda^2 - a\lambda}{2}\right) = 0.$$

Problem. Let A, B, C be three collinear points, B between A and C. On one side of line AC, we consider the equilateral triangle ACM, and on the other side of line AC, we consider the equilateral triangles ABP and BCR. Prove that the centroids of these triangles are the vertices of an equilateral triangle whose centroid lies on AC.

Solution. Let A be the origin of the complex plane and let $\overrightarrow{AC}$ be the positive real axis. If we denote $B(b)$, $C(c)$, then

$$P(-\omega^2 b), \ R(-b\omega - c\omega^2), \ M(-c\omega).$$

Further letting O_1, O_2, O_3 denote the respective centroids of triangles ACM, ABP, BCR, we have:

$$O_1\left(\frac{c - c\omega}{3}\right), \quad O_2\left(\frac{b - b\omega^2}{3}\right), \quad O_3\left(\frac{b + c - b\omega - c\omega^2}{3}\right)$$

and

$$\frac{c - c\omega}{3} + \frac{b + c - b\omega - c\omega^2}{3} \cdot \omega + \frac{b - b\omega^2}{3} \cdot \omega^2 = 0.$$

Finally, the centroid of triangle $O_1O_2O_3$ is

$$\frac{1}{3}\left(\frac{c - c\omega}{3} + \frac{b + c - b\omega - c\omega^2}{3} + \frac{b - b\omega^2}{3}\right) = \frac{b + c}{3} \in \mathbb{R},$$

so it lies on the real axis $\overrightarrow{AC}$.

Proposed Problems

1. Let $a, b, c \in \mathbb{C}$ be such that $|a| = |b| = |c| > 0$ and $a + b + c = 0$. Prove that a, b, c are the vertices of an equilateral triangle.

2. Let $a, b, c \in \mathbb{C}$ be such that
$$a\bar{b} = b\bar{c} = c\bar{a} \neq 0.$$
Prove that a, b, c are the vertices of an equilateral triangle.

3. Let $a, b, c \in \mathbb{C}^*$ be such that $a^2 = bc$ and $b^2 = ca$. Prove that a, b, c are the vertices of an equilateral triangle.

4. Let $a, b, c \in \mathbb{C}$ be three nonzero complex numbers of equal absolute value such that each of the following quadratic equations
$$az^2 + bz + c = 0 \quad , \quad bz^2 + cz + a = 0$$
has at least one solution with absolute value 1. Prove that a, b, c are the vertices of an equilateral triangle.

5. Let ABC be an equilateral triangle inscribed in a circle of radius R. Prove that for all points M on the circle,
$$MA^2 + MB^2 + MC^2 = 6R^2.$$

6. Let ABC be a triangle and $M, N \in AB$, $P, Q \in BC$, $R, S \in CA$ so that
$$AM = MN = NB \ , \ BP = PQ = QC \ , \ CR = RS = SA.$$
In the exterior of the triangle ABC, we consider again the equilateral triangles MNC', PQA', RSB'. Prove that the triangle $A'B'C'$ is equilateral.

7. Let $ABCD$ be a quadrilateral such that $AD = BC$ and $\angle C + \angle D = 2\pi/3$. We consider the equilateral triangles ACP, DCQ, DBR away from CD. Prove that the points P, Q, R are collinear.

8. Inside the quadrilateral $ABCD$, we consider the equilateral triangles ABM, CDP and outside $ABCD$, we consider the equilateral triangles BCN, DAQ. Prove that the points M, N, P, Q are the vertices of a parallelogram.

9. In the exterior of the triangle ABC, we consider the equilateral triangles ABM and ACN. Prove that the midpoints P, Q, R of the segments BC, AN, AM are the vertices of an equilateral triangle.

10. In the exterior of the triangle ABC, we consider the equilateral triangles ABM, ACN. Let P be the reflection of the point A relative to the midpoint of BC. Prove that the triangle MNP is equilateral.

11. In the exterior of the triangle ABC, we consider the equilateral triangles ABP, BCM, CAN. Let M' be the reflection of the point M relative to A. Prove that the triangle $M'NP$ is equilateral.

12. Let XAB, YCD, and ZEF be equilateral triangles with the same orientation, and let M, N, P, Q, R, and S be the midpoints of the line segments BC, DE, FA, AD, BE, and CF respectively.

    a) Show that if triangle XYZ is equilateral with the same orientation as XAB, YCD, and ZEF, then triangle MNP is equilateral.

    b) Show that if triangle XYZ is equilateral, and if XYZ and XAB have opposite orientation, then triangle QRS is equilateral.

13. Let ACE and BDF be equilateral triangles in the plane having the same orientation, and let M, N, P, Q, R, and S be the midpoints of the line segments BC, DE, FA, AD, BE, and CF respectively. Prove that triangles MNP and QRS are also equilateral.

14. Let $ABCDEF$ be a hexagon inscribed in a circle of center O such that

    $$\angle AOB = \angle COD = \angle EOF = \alpha.$$

    Let M, N, P be the respective midpoints of the sides BC, DE, AF. Prove that if the triangle MNP is equilateral and the triangle ACE is not equilateral, then $\alpha = \pi/3$.

15. Let $ABCDEF$ be a hexagon inscribed in a circle. Let M, N, P be the midpoints of the line segments BC, DE, and FA, respectively, and let Q, R, S be the midpoints of the line segments AD, BE, and CF, respectively. Show that if both triangles MNP and QRS are equilateral, then $AB = CD = EF$.

16. Let BCA', CAB', and ABC' be equilateral triangles constructed on the sides of a given triangle ABC, all towards the exterior (or all towards the interior) of ABC. Prove that $A'B'C'$ is also equilateral.

17. Let A', B', C', and D' be the centers of the squares erected outwards the quadrilateral $ABCD$ on the sides AB, BC, CD, and DA, respectively. Prove that $A'C'$ and $B'D'$ are perpendicular and have equal lengths.

18. Let OAM, OBN, OCP, and ODQ be right-angled, isosceles, and identically oriented triangles in the same plane, with hypotenuses OA, OB, OC, respectively OD. Let X, Y, Z, and T be the centroids of the triangles ANP, BPQ, CQM, respectively DMN.

    Show that the line segments XZ and YT are perpendicular and have equal lengths.

Solutions

1. **Solution I.** Let $z = \frac{b}{c}$. We have

$$|z| = \left|\frac{b}{c}\right| = \frac{|b|}{|c|} = 1,$$

$$|z+1| = \left|\frac{b}{c}+1\right| = \left|\frac{b+c}{c}\right| = \left|\frac{-a}{c}\right| = \frac{|-a|}{|c|} = 1.$$

If $z = x + iy$, $x, y \in \mathbb{R}$, then

$$\begin{cases} |z| = 1 \\ |z+1| = 1 \end{cases} \Rightarrow \begin{cases} x^2 + y^2 = 1 \\ (x+1)^2 + y^2 = 1 \end{cases}$$

By subtracting, $x = -\frac{1}{2}$ and then $y^2 = \frac{3}{4}$. We deduce that $z = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$, so $\left(\frac{b}{c}\right)^3 = 1$. Similarly, $\left(\frac{a}{c}\right)^3 = 1$. It follows that $a^3 = b^3 = c^3$. The numbers a, b, c are pairwise different, so we may assume that $b = \omega a$, $c = \omega^2 a$, with $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Solution II. We have

$$0 = \overline{a+b+c} = \bar{a} + \bar{b} + \bar{c} = \frac{|a|^2}{a} + \frac{|b|^2}{b} + \frac{|c|^2}{c}$$

$$\Rightarrow \frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 0 \Rightarrow ab + bc + ca = 0.$$

Further, $a^2 + b^2 + c^2 = (a+b+c)^2 - 2(ab+bc+ca) = 0$. Hence

$$a^2 + b^2 + c^2 = ab + bc + ca \ (= 0)$$

and the conclusion follows.

2. We have

$$\left|a\overline{b}\right| = |b\overline{c}| = |c\overline{a}| \Rightarrow |a| \cdot |b| = |b| \cdot |c| = |c| \cdot |a|,$$

so $|a| = |b| = |c|$. Without loss of generality, assume that each of these absolute values is equal to 1. Then

$$a\overline{b} = b\overline{c} = c\overline{a} \Rightarrow \frac{a}{b} = \frac{b}{c} = \frac{c}{a}$$

$$\Rightarrow a^2 = bc\ ,\ b^2 = ca\ ,\ c^2 = ab \Rightarrow a^2 + b^2 + c^2 = ab + bc + ca.$$

3. By dividing the given relations, we obtain $a^3 = b^3$. Then

$$c^2 = \frac{b^4}{a^2} = \frac{b \cdot b^3}{a^2} = \frac{b \cdot a^3}{a^2} = ab.$$

Finally, $a^2 + b^2 + c^2 = ab + bc + ca$.

4. If $|z| = 1$ and $az^2 + bz + c = 0$, then

$$0 = \overline{az^2 + bz + c} = \overline{a} \cdot \overline{z}^2 + \overline{b} \cdot \overline{z} + \overline{c} = \frac{|a|^2}{a} \cdot \frac{1}{z^2} + \frac{|b|^2}{b} \cdot \frac{1}{z} + \frac{|c|^2}{c}$$

$$\Rightarrow \frac{1}{az^2} + \frac{1}{bz} + \frac{1}{c} = 0 \Rightarrow \frac{1}{c}z^2 + \frac{1}{b}z + \frac{1}{a} = 0 \Rightarrow abz^2 + acz + bc = 0$$

$$\Rightarrow b(-bz - c) + acz + bc = 0 \Rightarrow (ac - b^2)z = 0 \Rightarrow b^2 = ac.$$

Analogously, $c^2 = ab$, and the conclusion follows.

5. Assume that $R = 1$ and $A(1)$, $B(\omega)$, $C(\omega^2)$, $M(z)$, with $|z| = 1$. We have

$$MA^2 + MB^2 + MC^2 = |z-1|^2 + |z-\omega|^2 + \left|z-\omega^2\right|^2$$

$$= (z-1) \cdot \overline{z-1} + (z-\omega) \cdot \overline{z-\omega} + (z-\omega^2) \cdot \overline{z-\omega^2}$$

$$= (z-1)\left(\frac{1}{z} - 1\right) + (z-\omega)\left(\frac{1}{z} - \omega^2\right) + (z-\omega^2)\left(\frac{1}{z} - \omega\right)$$

$$= 6 - z\left(1 + \frac{1}{\omega} + \frac{1}{\omega^2}\right) - \frac{1}{z}(\omega^2 + \omega + 1) = 6.$$

6. If we denote $A(a)$, $B(b)$, $C(c)$, then

$$M\left(\frac{2a+b}{3}\right),\ N\left(\frac{2b+a}{3}\right),$$

$$P\left(\frac{2b+c}{3}\right),\ Q\left(\frac{2c+b}{3}\right),$$

$$R\left(\frac{2c+a}{3}\right),\ S\left(\frac{2a+c}{3}\right).$$

Hence

$$A'\left(-\frac{2c+b}{3}\omega-\frac{2b+c}{3}\omega^2\right),$$

$$B'\left(-\frac{2a+c}{3}\omega-\frac{2c+a}{3}\omega^2\right),$$

$$C'\left(-\frac{2b+a}{3}\omega-\frac{2a+b}{3}\omega^2\right).$$

7. Let us consider the complex plane with the origin $O = AD\cap BC$ and let $\overrightarrow{OD}$ be the positive real semi-axis. Suppose, without loss of generality, that $AD = BC = 1$. We have: $A(a)$, $D(a+1)$, with $a\in\mathbb{R}$. $\angle DOC = \pi/3$, so $B(\lambda x)$, $C(\lambda x+\lambda)$, for some real x and $\lambda = \cos\frac{\pi}{3}+i\sin\frac{\pi}{3}$. Further,

$$p = -\lambda^2 a+\lambda^2 x+\lambda^2\ ,\ q = -\lambda^2(a+1)+\lambda^2 x+\lambda^2\ ,\ r = -(a+1)\lambda^2+\lambda^2 x.$$

Now, $\frac{r-q}{r-p}$ is real, hence P, Q, R are collinear.

8. If we denote $A(a)$, $B(b)$, $C(c)$, $D(d)$, then

$$M(-\omega a-\omega^2 b),\ N(-\omega c-\omega^2 b),\ P(-\omega c-\omega^2 d),\ Q(-\omega a-\omega^2 d).$$

We have

$$\frac{(-\omega a-\omega^2 b)+(-\omega c-\omega^2 d)}{2}=\frac{(-\omega c-\omega^2 b)+(-\omega a-\omega^2 d)}{2},$$

so the diagonals of the quadrilateral $MNPQ$ have the same midpoint, hence the conclusion follows.

9. If we assume $A(a)$, $B(b)$, $C(c)$, then

$$M(-\omega b-\omega^2 a),\ N(-\omega a-\omega^2 c).$$

Further, $P\left(\frac{b+c}{2}\right)$, $Q\left(\frac{a-\omega a-\omega^2 c}{2}\right)$, $R\left(\frac{a-\omega b-\omega^2 a}{2}\right)$ and

$$\frac{b+c}{2}+\frac{a-\omega a-\omega^2 c}{2}\cdot\omega+\frac{a-\omega b-\omega^2 a}{2}\cdot\omega^2=0,$$

meaning that PQR is equilateral.

10. If we denote $A(a)$, $B(b)$, $C(c)$, then

$$m = -\omega b - \omega^2 a \quad , \quad n = -\omega a - \omega^2 c.$$

The quadrilateral $ABPC$ is a parallelogram, so

$$a + p = b + c \Rightarrow p = b + c - a.$$

Now,

$$\begin{aligned} p + \omega n + \omega^2 m &= (b + c - a) + \omega(-\omega a - \omega^2 c) + \omega^2(-\omega b - \omega^2 a) \\ &= b + c - a - \omega^2 a - c - b - \omega a = 0, \end{aligned}$$

and the conclusion follows.

11. With $A(a)$, $B(b)$, $C(c)$, we have

$$M(-c\omega - b\omega^2)\ ,\ N(-a\omega - c\omega^2)\ ,\ P(-b\omega - a\omega^2)$$

and $M'(2a + c\omega + b\omega^2)$. The identity $m' + p\omega + n\omega^2 = 0$ is now easy to check.

12. Without loss of generality, we may suppose that triangles XAB, YCD, and ZEF are directly oriented.
Then we have (for $\omega = \cos(2\pi/3) + i\sin(2\pi/3)$)

$$x + a\omega + b\omega^2 = 0, \quad y + c\omega + d\omega^2 = 0, \quad \text{and} \quad z + e\omega + f\omega^2 = 0.$$

a) In this case, we have $x + y\omega + z\omega^2 = 0$. Add the above relations multiplied with 1, ω, and ω^2 respectively in order to obtain

$$(a + c\omega + e\omega^2)\omega + (b + d\omega + f\omega^2)\omega^2 = 0,$$

or (after multiplying by ω and using $\omega^3 = 1$)

$$(a + c\omega + e\omega^2)\omega^2 + (b + d\omega + f\omega^2) = 0.$$

But this can also be written in the form

$$\frac{b+c}{2} + \frac{d+e}{2}\omega + \frac{f+a}{2}\omega^2 = 0$$

which means that triangle MNP is equilateral (since $m = (b + c)/2$, $n = (d + e)/2$, and $p = (f + a)/2$).

b) Similarly, we now have $x + y\omega^2 + z\omega = 0$, thus if we multiply the equations from the beginning with 1, ω^2, and ω respectively, we get

$$(a + c\omega^2 + e\omega)\omega + (b + d\omega^2 + f\omega)\omega^2 = 0.$$

One can immediately note (by using the properties of ω) that this is equivalent to

$$\frac{a+d}{2}+\frac{b+e}{2}\omega+\frac{c+f}{2}\omega^2=0,$$

that is with $q+r\omega+s\omega^2=0$, proving that triangle QRS is equilateral.

Note that when points X, Y, and Z coincide, say $X=Y=Z=O$, we get the following nice statement: if triangles OAB, OCD, and OEF are equilateral and have the same orientation, then triangles MNP and QRS are both equilateral (with M, N, P, Q, R, S defined above), because triangle XYZ is reduced to one point, its orientation can be considered anyhow. This is a statement that we met before (see one of the solved problems) with a slightly different worded solution. Also note the particular case: if $ABCDEF$ is a hexagon inscribed in a circle of radius R, and $AB=CD=EF=R$, then triangles MNP and QRS are both equilateral (using the same M, N, P, Q, R, S from above). For this one point, O is, of course, the center of the circle.

13. Suppose ACE and BDF have positive orientation, and, as usual, let $\omega=\cos(2\pi)/3+i\sin(2\pi/3)$. We thus have

$$a+c\omega+e\omega^2=0 \text{ and } b+d\omega+f\omega^2=0.$$

Consequently,

$$\frac{b+c}{2}+\frac{d+e}{2}\omega+\frac{f+a}{2}\omega^2=\frac{1}{2}\left((a+c\omega+e\omega^2)\omega^2+(b+d\omega+f\omega^2)\right)=0,$$

and thus,

$$\frac{a+d}{2}+\frac{b+e}{2}\omega^2+\frac{c+f}{2}\omega=\frac{1}{2}\left((a+c\omega+e\omega^2)+(b+d\omega+f\omega^2)\omega^2\right)=0,$$

meaning that MNP and QRS are equilateral. Observe that, unlike in the previous problem, triangles MNP and QRS now have opposite orientations. For the case of a hexagon $ABCDEF$ inscribed in a circle, we will see further some converse statements.

14. Assume that $A(a)$, $C(c)$, $E(e)$, and let $\lambda=\cos\alpha+i\sin\alpha$. Then

$$b=\lambda a, \quad d=\lambda c, \quad f=\lambda e.$$

The triangle MNP is equilateral, so

$$m+n\omega+p\omega^2=0\Rightarrow\frac{a\lambda+c}{2}+\omega\cdot\frac{c\lambda+e}{2}+\omega^2\cdot\frac{e\lambda+a}{2}=0$$
$$\Rightarrow\lambda(a+c\omega+e\omega^2)+(a+c\omega+e\omega^2)\omega^2=0.$$

But $a + c\omega + e\omega^2 \neq 0$, because the triangle ACE is not equilateral, thus

$$\lambda = -\omega^2 \Rightarrow \alpha = \pi/3.$$

15. Let $\omega = \cos(2\pi/3) + i\sin(2\pi/3)$ and let us denote by the small corresponding letters the affixes of the points, that is, a is the complex number represented in A, and so on. Then, of course, we have $m = (b+c)/2$, $n = (d+e)/2, p = (f+a)/2, q = (a+d)/2, r = (b+e)/2$, and $s = (c+f)/2$. Assume first that triangles MNP and QRS have the same orientation (say positive, without loss of generality). So, because these triangles are equilateral and directly oriented, we have $m + n\omega + p\omega^2 = 0$ and $q + r\omega + s\omega^2 = 0$. The first of these equalities gives us

$$(b+c) + (d+e)\omega + (f+a)\omega^2 = 0$$

which can be also written as

$$(a + b\omega) + (c + d\omega)\omega + (e + \omega f)\omega^2 = 0$$

after multiplication by ω (do not forget $\omega^3 = 1$!).

Similarly, $q + r\omega + s\omega^2 = 0$ leads to the equality

$$(a+d) + (b+e)\omega + (c+f)\omega^2 = 0,$$

which is immediately seen to be equivalent to

$$(a + b\omega) + (c + d\omega)\omega^2 + (e + \omega f)\omega = 0.$$

Now there is no problem to see that $x + y\omega + z\omega^2 = 0$ and $x + y\omega^2 + z\omega = 0$ together imply $x = y = z$ (with the aid of $1 + \omega + \omega^2 = 0$). In our case, the equalities

$$a + b\omega = c + d\omega = e + f\omega$$

follow.

But $a + b\omega = c + d\omega$, or $a - c = (d - b)\omega$ shows that AC and BD are of equal length, which implies either $AB = CD$, or $AB \parallel CD$ (as A, B, C, and D belong to the same circle). Similarly, $a + b\omega = e + f\omega$ implies $AE = BF$, thus either $AB = EF$, or $AB \parallel EF$, and from $c + d\omega = e + f\omega$, we infer $CE = DF$, yielding either $CD = EF$, or $CD \parallel EF$. Now, since we cannot have $AB \parallel CD \parallel EF$, at most one of the relations $AB \parallel CD$, $AB \parallel EF$, and $CD \parallel EF$ can hold, therefore at least two of $AB = CD$, $AB = EF$, and $CD = EF$ must be true. That is, the equalities $AB = CD = EF$ surely follow.

Prove that in this situation, each of AB, CD, and EF is actually equal to the radius of the circle that circumscribes $ABCDEF$ — that is, triangles OAB, OCD, and OEF are equilateral, O being the center of the circle. (Note that $a - c = (d - b)\omega$ gives the angle between AC and BD, etc.)

In the second case (when MNP and QRS have opposite orientations), we get

$$(b + c) + (d + e)\omega + (f + a)\omega^2 = 0$$

and

$$(a + d) + (b + e)\omega^2 + (c + f)\omega = 0,$$

and we can rewrite these as

$$(a + c\omega + e\omega^2)\omega^2 + (b + d\omega + f\omega^2) = 0$$

and

$$(a + c\omega + e\omega^2) + (b + d\omega + f\omega^2)\omega^2 = 0,$$

respectively. But $x\omega^2 + y = 0$ and $x + y\omega^2 = 0$ imply $x = y = 0$. In our case, we obtain

$$a + c\omega + e\omega^2 = 0 \text{ and } b + d\omega + e\omega^2 = 0,$$

meaning that triangles BDF and ACE are equilateral, which leads again to $AB = CD = EF$ (using the fact that A, B, C, D, E, F are on the same circle). This is problem 11470 from *The American Mathematical Monthly.*

16. Consider the case when A', B', and C' are in the exterior of ABC. If ABC is directly oriented, we have

$$a' = \frac{b - c\omega}{1 - \omega},\quad b' = \frac{c - a\omega}{1 - \omega},\quad \text{and}\quad c' = \frac{a - b\omega}{1 - \omega},$$

with $\omega = \cos(2\pi/3) + i\sin(2\pi/3)$. Thus,

$$a' + b'\omega + c'\omega^2 = \frac{1}{1 - \omega}(b - c\omega + c\omega - a\omega^2 + a\omega^2 - b) = 0,$$

leading to the desired conclusion. We proceed similarly in the case of triangles oriented towards the interior of ABC.

Note that the equilateral triangles $A'B'C'$ thus obtained are called Napoleon's triangles. Try to prove (possibly by using complex numbers) that the square of the length of the side of the exterior Napoleon triangle is

$$\frac{1}{6}(BC^2 + CA^2 + AB^2 + 4S\sqrt{3})$$

while for the interior triangle, this magnitude equals

$$\frac{1}{6}(BC^2 + CA^2 + AB^2 - 4S\sqrt{3}).$$

And thus we get Weitzenböck's inequality $BC^2 + CA^2 + AB^2 \geq 4S\sqrt{3}$ for every triangle ABC with area S (with equality if and only if the triangle is equilateral).

17. Why only equilateral triangles? We can work in the same way with squares, or right isosceles triangles, or any other isosceles triangle (as we have seen in the previous problem). If $ABCD$ is directly oriented we have $a' - a = (a' - b)i$, hence

$$a' = \frac{a - bi}{1 - i},$$

and, analogously,

$$b' = \frac{b - ci}{1 - i}, \quad c' = \frac{c - di}{1 - i}, \quad \text{and } d' = \frac{d - ai}{1 - i}.$$

(We always keep the same convention that a stands for the number represented in A, and so on.) Consequently,

$$d' - b' = \frac{1}{1 - i}(-ai - b + ci + d) = i(c' - a'),$$

that is, $A'C'$ and $B'D'$ are perpendicular and congruent.

Does the result remain true if the squares are built inwards with respect to the quadrilateral $ABCD$?

Remark. There is a nice synthetic proof of this result, based on the fact that if both right isosceles triangles OXY and OZT have the right angles in O, and they have the same orientation, then XZ and YT are perpendicular and congruent (observe the rotation!).

In our problem, we choose O to be the midpoint of AC. Using the above mentioned fact and the properties of the midline in a triangle, one can show that triangles $OA'B'$ and $OC'D'$ are right isosceles, and the conclusion follows. (Of course, a similar proof works if one considers the midpoint of BD.)

18. We consider a Cartesian coordinate system with origin O. Then, as one can immediately see, we have

$$m = (1 + i)a/2, \quad n = (1 + i)b/2, \quad p = (1 + i)c/2, \quad q = (1 + i)d/2,$$

hence

$$x = \frac{1}{3}\left(a + \frac{1+i}{2}b + \frac{1+i}{2}c\right), \quad y = \frac{1}{3}\left(b + \frac{1+i}{2}c + \frac{1+i}{2}d\right),$$

$$z = \frac{1}{3}\left(c + \frac{1+i}{2}d + \frac{1+i}{2}a\right), \quad t = \frac{1}{3}\left(d + \frac{1+i}{2}a + \frac{1+i}{2}b\right).$$

It follows that

$$z - x = \frac{1}{3}\left(-\frac{1-i}{2}a - \frac{1+i}{2}b + \frac{1-i}{2}c + \frac{1+i}{2}d\right)$$

$$t - y = \frac{1}{3}\left(\frac{1+i}{2}a - \frac{1-i}{2}b - \frac{1+i}{2}c + \frac{1-i}{2}d\right),$$

consequently $z - x = i(t - y)$, and the problem is solved.

Chapter 11

Recurrence Relations

One method to define a sequence $(x_n)_{n\geq 1}$ is to express each term of the sequence as a function of some previous terms. For example, a sequence can be defined if it is given a function $f : \mathbb{R} \to \mathbb{R}$ so that

$$x_{n+1} = f(x_n), \tag{1}$$

for all integers $n \geq 1$, and also the first term of the sequence. The recurrence (1) is a *recurrence of the first order.* In particular,

$$x_{n+1} = ax_n + b, \tag{2}$$

for some real numbers a, b, $a \neq 0$, is called a *linear recurrence of the first order.* In case $a = 1$, the sequence $(x_n)_{n\geq 1}$ is an arithmetic progression. If $a \neq 1$, we always can find a real number α such that the sequence $y_n = x_n + \alpha$ is geometric progression. Indeed, we have

$$\frac{y_{n+1}}{y_n} = \frac{x_{n+1} + \alpha}{x_n + \alpha} = \frac{ax_n + b + \alpha}{x_n + \alpha} = a + \frac{b + (1-a)\alpha}{x_n + \alpha} = a,$$

as long as

$$b + (1-a)\alpha = 0, \text{ so } \alpha = \frac{b}{a-1}.$$

A recurrence relation of the form

$$ax_{n+2} + bx_{n+1} + cx_n = 0, \tag{3}$$

for $n \geq 1$, with given x_1, x_2, is called a *linear recurrence of the second order.* If $\lambda_1, \lambda_2 \in \mathbb{C}$, $\lambda_1 \neq \lambda_2$ are the solutions of the associated quadratic equation

$$a\lambda^2 + b\lambda + c = 0,$$

then easily, any sequences

$$y_n = C\lambda_1^n \text{ and } z_n = C\lambda_2^n$$

satisfy the recurrence (3), where $C \in \mathbb{R}$. It can be proved that the general term of the sequence $(x_n)_{n\geq 1}$ is given by the formula

$$x_n = \alpha\lambda_1^n + \beta\lambda_2^n,$$

for all integers $n \geq 1$ and for some α and β, but only under the hypothesis that $\lambda_1 \neq \lambda_2$. If $\lambda_1 = \lambda_2$, the general formula for x_n is best written in the form

$$x_n = \alpha n\lambda_1^{n-1} + \beta\lambda_1^n,$$

for some α and β. Analogously, a *linear recurrence of order k* is one of the form

$$a_0x_n + a_1x_{n+1} + \ldots + a_kx_{n+k} = 0.$$

The associated polynomial

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_kx^k$$

has roots $z_1, z_2, \ldots, z_k$. In case $z_i \neq z_j$ for all $i \neq j$, our sequence is once again of the form

$$x_n = \alpha_1z_1^n + \alpha_2z_2^n + \ldots + \alpha_kz_k^n,$$

for some α_i.

All these are consequences of the following general result:

Theorem. *i) If a sequence of complex numbers* $(u_n)_{n\geq 1}$ *satisfies a linear recurrence with constant coefficients, then* $f(z) = \sum_{n\geq 0} u_nz^n$ *is a rational fraction in a neighborhood of* 0.

ii) Suppose that a sequence satisfies a relation of the form

$$u_{n+h} = q_1u_{n+h-1} + q_2u_{n+h-2} + \ldots + q_hu_n,$$

where

$$Q(X) = 1 - q_1X - \ldots - q_hX^h = (1-\alpha_1X)^{m_1}(1-\alpha_2X)^{m_2}\ldots(1-\alpha_sX)^{m_s}$$

is the factorization of Q *in* $\mathbb{C}[X]$. *Then there exist complex polynomials* $P_1, P_2, \ldots, P_s$ *such that* $\deg(P_i) < m_i$ *and*

$$u_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \ldots + P_s(n)\alpha_s^n.$$

The proof is not very difficult, though quite technical. Let us start with the first assertion. Assume that the sequence $(u_n)_{n\geq 1}$ satisfies the relation

$$u_{n+h} = q_1 u_{n+h-1} + q_2 u_{n+h-2} + \ldots + q_h u_n$$

and consider $M = \max(|q_1|, |q_2|, \ldots, |q_h|)$. Then, using the triangle inequality, we deduce that

$$|u_{n+h}| \leq M(|u_n| + |u_{n+1}| + \ldots + |u_{n+h-1}|).$$

Let $C > \max(|u_0|, |u_1|, \ldots, |u_h|, 1)$ and let $A > 1 + M$.
We claim that $|u_n| \leq CA^n$ for all n. This is clear for $n \leq h$. Assuming it is true for all values smaller than $n + h$, the previous inequality allows us to write

$$|u_{n+h}| \leq MCA^n(1 + A + \ldots + A^{h-1}) < \frac{MC}{A-1}A^{n+h} < CA^{n+h},$$

which finishes the inductive proof. This shows that $|u_n| \leq CA^n$ for all n and proves that the series $\sum\limits_{n\geq 0} u_n z^n = f(z)$ converges absolutely for $|z| < \dfrac{1}{A}$.
Because $(u_n)_{n\geq 1}$ satisfies the relation in the statement of the theorem, all coefficients of z^k in $Q(z)f(z)$ are zero for $k \geq h$. Thus, in some neighborhood V of 0, we have the existence of a polynomial P of degree smaller than h such that $f(z) = \dfrac{P(z)}{Q(z)}$ for all $z \in V$.

In order to prove the second statement, we will use i). Write

$$f(z) = \frac{P(z)}{Q(z)} \quad \text{for} \quad z \in V.$$

On the other hand, a well-known result asserts the existence of numbers r_{ij} such that

$$\frac{P(z)}{Q(z)} = \sum_{i=1}^{s}\sum_{j=1}^{m_i} \frac{r_{ij}}{(1-\alpha_i z)^j}.$$

The identity

$$\frac{1}{(1-Y)^j} = \sum_{r\geq 0}\binom{r+j-1}{j-1}Y^r,$$

obtained by differentiating $j-1$ times the relation

$$1 + Y + Y^2 + \ldots = \frac{1}{1-Y},$$

shows that

$$\frac{P(z)}{Q(z)} = \sum_{r\geq 0}\left(\sum_{i=1}^{s}\sum_{j=1}^{m_i} r_{ij}\binom{r+j-1}{j-1}\alpha_i^r\right) z^r.$$

Thus

$$u_n = \sum_{i=1}^{s}\sum_{j=1}^{m_i} r_{ij}\binom{n+j-1}{j-1}\alpha_i^n,$$

which finishes the proof of the theorem.

Recurrence relations are sometimes useful in solving functional equations. Here is a quite challenging example, from Gazeta Matematica's contest:

Problem. Find all monotone functions $f : \mathbb{R} \to \mathbb{R}$ such that

$$f(f(f(x))) - 3f(f(x)) + 6f(x) = 4x + 3$$

for all real numbers x.

Solution. Let x be an arbitrary real number and define the sequence x_n by $x_0 = x$ and $x_n = f(x_{n-1})$. The relation in the statement of the problem gives

$$x_{n+3} - 3x_{n+2} + 6x_{n+1} = 4x_n + 3.$$

Consider the sequence $a_n = x_n - n$. Then we have

$$a_{n+3} - 3a_{n+2} + 6a_{n+1} - 4a_n = 0$$

for all n. Because the equation $t^3 - 3t^2 + 6t - 4 = 0$ has the solutions 1, $2e^{\frac{i\pi}{3}}$, $2e^{-\frac{i\pi}{3}}$, it follows that there exist functions A, B, C such that

$$y_n = A(x) + 2^n\left(B(x)\cos\left(\frac{n\pi}{3}\right) + C(x)\sin\left(\frac{n\pi}{3}\right)\right).$$

From the relation satisfied by f, it follows immediately that f is injective, so actually f is strictly increasing (it is clear that if f is decreasing, then $f(f(f(x))) - 3f(f(x)) + 6f(x)$ is decreasing).

Now, let $x < y$. Because $f^n(x) < f^n(y)$ for all n (where f^n denotes the composition of f with itself n times), it follows that

$$(B(x) - B(y))\cos\left(\frac{n\pi}{3}\right) + (C(x) - C(y))\sin\left(\frac{n\pi}{3}\right) > \frac{A(x) - A(y)}{2^n}.$$

By writing the same relation for $n + 3$, we immediately deduce that

$$(B(x) - B(y))\cos\left(\frac{n\pi}{3}\right) + (C(x) - C(y))\sin\left(\frac{n\pi}{3}\right) = 0$$

for all n, which implies that the functions B, C are constant, equal to some b, c. Because

$$f^n(x) = A(x) + 2^n\left(b\cos\left(\frac{n\pi}{3}\right) + c\sin\left(\frac{n\pi}{3}\right)\right)$$

for all n and all x, we easily deduce by taking $n = 0$ and $n = 1$ that $f(x) = x+1$ for all x.

Let us say a few words about homographic sequences. These are sequences satisfying relations of the form

$$x_{n+1} = \frac{ax_n + b}{cx_n + d}.$$

We can actually compute the general term of such a sequence. Let us suppose that $ad \neq bc$, the other case being trivial.
Let us search for x_n a formula $x_n = \dfrac{y_n}{z_n}$. Then

$$\frac{y_{n+1}}{z_{n+1}} = \frac{ay_n + bz_n}{cy_n + dz_n}.$$

We then impose

$$\begin{cases} y_{n+1} = ay_n + bz_n \\ z_{n+1} = cy_n + dz_n \end{cases}.$$

These relations imply that $(y_n)_{n\geq 1}$ and $(z_n)_{n\geq 1}$ satisfy second order recurrence relations, and thus their general terms can be explicitly computed. From here, we find the general term of $(x_n)_{n\geq 1}$.

It should not seem unnatural that a sequence satisfying a recurrence of order k and having only a finite number of distinct terms is periodic. This will be the key argument in the following example, taken from a Romanian National Olympiad.

Problem. Let $z_1, z_2, \ldots, z_n$ be complex numbers such that the sequence

$$u_k = z_1^k + z_2^k + \ldots + z_n^k$$

takes only a finite number of values. Prove that $(u_k)_{k\geq 1}$ is periodic.

Solution. The main theorem of this chapter shows that u_k satisfies a recurrence of order n. This can be also directly established: if

$$S_1 = \sum_{i=1}^{n} z_i,\ S_2 = \sum_{1\leq i<j\leq n} z_i z_j, \ldots,\ S_n = z_1 \ldots z_n,$$

then

$$z_i^n - z_i^{n-1}S_1 + z_i^{n-2}S_2 + \ldots + (-1)^n S_n = 0$$

for all $1 \leq i \leq n$.
By multiplying by z_i^k and adding up these relations, we obtain

$$u_{n+k} - S_1 u_{n+k-1} + \ldots + (-1)^n S_n u_k = 0.$$

Now, suppose that $(u_k)_{k\geq 1}$ takes only finitely many values. Then so does the sequence of n-tuples $(u_k, u_{k+1}, \dots, u_{k+n-1})$. Thus there are $i < j$ such that $u_i = u_j$, $u_{i+1} = u_{j+1}, \dots,$ $u_{i+n-1} = u_{j+n-1}$. The recurrence relation immediately implies that the sequence $(u_k)_k$ becomes periodic with period $j - i$.

Unfortunately, in most of the cases we cannot find the general term of a sequence, even in case of the easiest recurrence relation $x_{n+1} = f(x_n)$. Usually, in these cases, we are interested in the asymptotic behavior of the sequence and, in particular, we would like to study its convergence. Clearly, if f is continuous and $(x_n)_{n\geq 1}$ converges, then the limit is a fixed point of f. Also, if we manage to find an interval I such that $f(I) \subset I$ and f increases on I, then if we can find n_0 such that $x_{n_0} \in I$, the sequence $(x_n)_n$ will rest in I for $n \geq n_0$ and will become monotone. If I is also bounded, then $(x_n)_n$ will converge. However, things are much more complicated in practice, as the following example shows.

Problem. Study the sequence $(x_n)_{n\geq 0}$ where $x_0 \in \mathbb{R}$ and

$$x_{n+1} = 2x_n^2 - 1.$$

In particular, find those x_0 for which the sequence converges and find its limit in this case. Also, find a closed form for x_n.

Solution. An easy case is when $|x_0| > 1$. Then it easily follows by induction that $x_n > 1$ for $n \geq 1$, and since

$$x_{n+1} - x_n = (2x_n + 1)(x_n - 1) > 0,$$

the sequence is increasing.

We conclude that $\lim_{n\to\infty} x_n = \infty$, because if $\lim_{n\to\infty} x_n = l \in \mathbb{R}$, then $l = 2l^2 - 1$, thus $l = -\frac{1}{2}$ or $l = 1$, which cannot happen because $l \geq x_1 > 1$. If we let

$$|x_0| = \frac{e^a + e^{-a}}{2},$$

then

$$x_1 = 2x_0^2 - 1 = \frac{e^{2a} + e^{-2a}}{2}$$

and by induction,

$$x_n = \frac{e^{2^n a} + e^{-2^n a}}{2},$$

where $a = \ln(|x_0| + \sqrt{x_0^2 - 1})$. Thus

$$x_n = \frac{(|x_0| + \sqrt{x_0^2 - 1})^{2^n} + (|x_0| - \sqrt{x_0^2 - 1})^{2^n}}{2}, \quad n \geq 1.$$

The more difficult case is when $x_0 \in (-1, 1)$ (the cases $x_0 = \pm 1$ are trivial). Let $a = \arccos x_0$; then an immediate induction shows that $x_n = \cos(2^n a)$.

Let us suppose that x_n converges to l. Then $l = 2l^2 - 1$, thus $l = -\dfrac{1}{2}$ or $l = 1$. Suppose that $l = 1$. Then

$$|x_{n+1} - 1| = 2|x_n - 1| \cdot |x_n + 1|,$$

thus $|x_{n+1} - 1| \geq 2|x_n - 1|$ for $n \geq n_0$. If $x_{n_0} \neq 1$, then

$$|x_n - 1| \geq 2^{n-n_0}|x_{n_0} - 1|,$$

which contradicts the fact that $\lim\limits_{n\to\infty} |x_n - 1| = 0$. Thus $x_{n_0} = 1$, and the sequence is constant from the rank n_0. Now, suppose that $l = -\dfrac{1}{2}$. Then

$$2x_{n+1} + 1 = (2x_n + 1)(2x_n - 1),$$

which implies

$$|2x_{n+1} + 1| \geq \frac{3}{2}|2x_n + 1|, \quad n \geq n_1.$$

Similarly, $x_{n_1} = -\dfrac{1}{2}$ and the sequence becomes constant from the rank n_1. Thus the sequence converges when $x_0 = \cos\dfrac{2k\pi}{2^n}$ for some n and $0 \leq k < 2^n$ or $x_0 = \cos\dfrac{2k\pi \pm \frac{2\pi}{3}}{2^m}$ for some m and $0 \leq k < 2^m$.

Proposed Problems

1. Let $(x_n)_{n\geq 1}$ be a sequence of real numbers defined by $x_1 \in (0, 1)$ and $x_{n+1} = x_n - x_n^2$ for all $n \geq 1$. Prove that:

   a) The sequence $(x_n)_{n\geq 1}$ converges to 0 and $\lim_{n\to\infty} nx_n = 1$.

   b) We have $\lim_{n\to\infty} \frac{n}{\ln n}(1 - nx_n) = 1$.

2. Let $x_0 = x_1 = 1$ and for any positive integer n,

$$x_{n+1} = \frac{x_n^2 + 1}{x_{n-1}}.$$

   Prove that x_n is an integer for all n.

3. Test for convergence the sequence $(x_n)_{n\geq 1}$ given by the recurrence relation

$$x_{n+1} = 3 + \frac{5}{x_n},\ n \geq 1.$$

4. Let $(x_n)_{n\geq 1}$ be a sequence of positive real numbers given by the recurrence relation
$$x_{n+1} = x_n + x_n^2,$$
for every positive integer n. Prove that there exists a positive real number α such that
$$\lim_{n\to\infty} \frac{x_n}{\alpha^{2^n}} = 1.$$

5. Consider the sequence $(a_n)_{n\geq 1}$ given by the formula
$$a_n = \left\lfloor (2+\sqrt{3})^n \right\rfloor.$$
Find a recurrence relation for the sequence $(a_n)_{n\geq 1}$.

6. Prove that for all k, there is an $\alpha \in \mathbb{R} - \mathbb{Q}$ such that
$$k \mid \lfloor \alpha^n \rfloor + 1$$
for all positive integers n.

7. Let $a, b > 0$. Find all $f : [0,\infty) \to [0,\infty)$ such that
$$f(f(x)) + af(x) = b(a+b)x,$$
for all $x \geq 0$.

8. Let us consider the Fibonacci sequence $(f_n)_{n\geq 1}$ given by the recurrence relation
$$f_{n+2} = f_{n+1} + f_n,$$
with $f_1 = f_2 = 1$. Find a linear recurrence relation for the sequence $(a_n)_{n\geq 1}$ given by the formula $a_n = f_n^2$.

9. Let us consider the Fibonacci sequence $(f_n)_{n\geq 1}$ given by the recurrence relation
$$f_{n+2} = f_{n+1} + f_n,$$
with $f_1 = f_2 = 1$. Prove that the sequence $(a_n)_{n\geq 1}$ given by the formula
$$a_n = \sum_{k=1}^{n} \frac{1}{f_k f_{k+2}},$$
for all nonnegative integers n, converges to 1.

10. Let a, b, c be real numbers and define the sequence $(a_n)_{n\geq 1}$ by the recurrence relation
$$a_{n+3} = \frac{1}{3}(a_{n+2} + a_{n+1} + a_n),$$
with $a_1 = a$, $a_2 = b$, $a_3 = c$. Prove that the sequence $(a_n)_{n\geq 1}$ converges to $(a + 2b + 3c)/6$.

11. For all $n \in \mathbb{N}$, let
$$S_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} 2005^k$$
Prove that $2^{n-1} \mid S_n$.

12. Let $1 = x_1, x_2, \ldots$ be a sequence of real numbers such that for all $n \geq 1$, we have
$$x_{n+1} = x_n + \frac{1}{2x_n}.$$
Prove that
$$\lfloor 25x_{625} \rfloor = 625.$$

13. Find all $f : \mathbb{N} \to \mathbb{N}$ such that
$$2n + 2001 \leq f(f(n)) + f(n) \leq 2n + 2002,$$
for all $n \in \mathbb{N}$.

14. Consider the sequence $(a_n)_{n\in\mathbb{N}}$ given by the recurrence relation
$$a_{n+3} = a_n + a_{n+1},$$
for every nonnegative integer n, with $a_0 = 3$, $a_1 = 0$, $a_2 = 2$. Prove that p divides a_p for every prime number p.

15. Let $m = 4k^2 - 5$, $k \geq 2$. Prove that there are $a, b \in \mathbb{N}$ such that the sequence $(x_n)_{n\geq 0}$ defined by $x_0 = a$, $x_1 = b$, and $x_{n+2} = x_{n+1} + x_n$ for $n \geq 0$ has all its elements relatively prime to m.

16. Given $a, b, c > 0$ with $b^2 > 4ac$, let $(\lambda_n)_{n\geq 0}$ be a sequence of real numbers, with $\lambda_0 > 0$ and $c\lambda_1 > b\lambda_0$. Let $u_0 = c\lambda_0$, $u_1 = c\lambda_1 - b\lambda_0$, and for $n \geq 2$, let $u_n = a\lambda_{n-2} - b\lambda_{n-1} + c\lambda_n$. Show that if $u_n > 0$ for all $n \geq 0$, then $\lambda_n > 0$ for all $n \geq 0$.

17. Let $(u_n)_{n\geq 1}$ be a sequence of real numbers defined by $u_1 = 1$ and
$$u_{n+1} = 1 + \frac{n}{u_n},$$

for all $n \geq 1$.

a) Prove that $\sqrt{n} \leq u_n < \sqrt{n} + 1$, for all $n \geq 1$.

b) Does the sequence $(u_n - \sqrt{n})_{n\geq 1}$ have a limit for $n \to \infty$?

Solutions

1. a) The convergence of the sequence $(x_n)_{n\geq 1}$ follows immediately, by two observations: the sequence is bounded (an obvious induction shows that $x_n \in (0,1)$ for all n) and strictly decreasing, because

$$x_{n+1} - x_n = -x_n^2 < 0$$

for all $n \geq 1$. Therefore, by the monotone convergence theorem for real sequences, $(x_n)_{n\geq 1}$ has a finite limit x. Passing to the limit in the recurrence relation, we get $x = x - x^2$, hence $x = 0$.

Alternatively, one can prove that $0 < x_n < 1/n$ for all $n \geq 1$, also inductively. Indeed, we have $0 < x_1 < 1$ and $0 < x_2 \leq 1/4 < 1/2$, because $x_2 \leq 1/4$ is equivalent to $(x_1 - 1/2)^2 \geq 0$, and $0 < x_1 < 1$ implies $x_2 > 0$. If, for $n \geq 2$, we have $0 < x_n < 1/n$, it follows that $x_n < 1/2$ as well. Because the quadratic function $x \mapsto x - x^2$ is increasing for $x \leq 1/2$, we get

$$x_{n+1} = x_n - x_n^2 < 1/n - (1/n)^2 = (n-1)/n^2 < 1/(n+1),$$

and $x_{n+1} > 0$, finishing the proof.

As we have

$$\lim_{n\to\infty} \frac{n+1-n}{\frac{1}{x_{n+1}} - \frac{1}{x_n}} = \lim_{n\to\infty} \frac{x_{n+1}}{x_n} = \lim_{n\to\infty} (1 - x_n) = 1$$

and the sequence with general term $1/x_n$ is strictly increasing and unbounded, we can apply the Stolz-Cesàro theorem to infer that

$$\lim_{n\to\infty} nx_n = \lim_{n\to\infty} \frac{n}{\frac{1}{x_n}} = 1,$$

as we intended to prove.

For part b), let us consider the sequence $(y_n)_{n\geq 1}$ with general term $y_n = 1/x_n - n$ and observe that

$$y_{n+1} - y_n = \frac{1}{x_{n+1}} - \frac{1}{x_n} - 1 = \frac{x_n}{1 - x_n},$$

therefore

$$\lim_{n\to\infty}(n+1)(y_{n+1}-y_n)=\lim_{n\to\infty}\frac{n+1}{n}\cdot nx_n\cdot\frac{1}{1-x_n}=1$$

(because of the above results: $\lim_{n\to\infty}x_n=0$ and $\lim_{n\to\infty}nx_n=1$). By the Stolz-Cesàro theorem we infer

$$\lim_{n\to\infty}\frac{y_n}{1+\frac{1}{2}+\cdots+\frac{1}{n}}=1,$$

and using the well-known fact that

$$\lim_{n\to\infty}\frac{1+\frac{1}{2}+\cdots+\frac{1}{n}}{\ln n}=1,$$

we get $\lim_{n\to\infty}y_n/\ln n=1$. This means that

$$\lim_{n\to\infty}\frac{1}{\ln n}\left(\frac{1}{x_n}-n\right)=1,$$

and consequently,

$$\lim_{n\to\infty}\frac{n}{\ln n}(1-nx_n)=\lim_{n\to\infty}\frac{1}{\ln n}\cdot\left(\frac{1}{x_n}-n\right)\cdot nx_n=1,$$

which is the required result.

2. We proceed by induction. Assume that $x_0,x_1,\ldots,x_n$ are integers. From

$$x_{n-2}x_n=x_{n-1}^2+1,$$

it follows that any two consecutive terms x_{n-2} and x_{n-1} are relatively prime. Now,

$$x_{n+1}=\frac{x_n^2+1}{x_{n-1}}=\frac{(x_{n-1}^2+1)^2+x_{n-2}^2}{x_{n-2}^2x_{n-1}},$$

so it is sufficient to prove that

$$x_{n-2}^2\mid N\quad\text{and}\quad x_{n-1}\mid N,$$

where

$$N=(x_{n-1}^2+1)^2+x_{n-2}^2.$$

Using the induction hypothesis, namely, that

$$x_n=\frac{x_{n-1}^2+1}{x_{n-2}},$$

is an integer, we deduce that x_{n-2} divides x_{n-1}^2+1. From the definition of N, we derive

$$x_{n-2}^2 \mid N.$$

Then

$$N \equiv 1 + x_{n-2}^2 \equiv x_{n-3}x_{n-1} \equiv 0 (\text{mod } x_{n-1}).$$

Note that we can also find the general term of this sequence. Indeed, by writing two consecutive relations

$$x_{n-1}x_{n+1} = x_n^2 + 1 \quad \text{and} \quad x_{n-2}x_n - x_{n-1}^2 = 1$$

and taking the difference, we conclude that

$$x_n(x_n + x_{n-2}) = x_{n-1}(x_{n-1} + x_{n+1}),$$

which can also be written as

$$\frac{x_{n-1} + x_{n+1}}{x_n} = \frac{x_{n-2} + x_n}{x_{n-1}},$$

which shows that the sequence $\frac{x_{n-1} + x_{n+1}}{x_n}$ is constant. Thus x_n will satisfy a second order linear recurrence.

3. Let us define

$$a_n = x_1x_2 \dots x_n \ , \quad n \geq 1.$$

Then $x_n = \frac{a_n}{a_{n-1}}$, for all integers $n \geq 2$, so the given relation can be written as

$$a_{n+1} - 3a_n = 5a_{n-1}.$$

The corresponding quadratic equation $\lambda^2 - 3\lambda - 5 = 0$ has the roots

$$\lambda_1 = \frac{3 + \sqrt{29}}{2} \ , \ \lambda_2 = \frac{3 - \sqrt{29}}{2},$$

so $a_n = \alpha\lambda_1^n + \beta\lambda_2^n$, for all positive integers n and for some real numbers α, β. If $\alpha\beta \neq 0$, then the sequence $(x_n)_{n\geq 1}$ is convergent,

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \frac{\alpha\lambda_1^n + \beta\lambda_2^n}{\alpha\lambda_1^{n-1} + \beta\lambda_2^{n-1}} = \lim_{n\to\infty} \frac{\lambda_1^n\left(\alpha + \beta\left(\frac{\lambda_2}{\lambda_1}\right)^n\right)}{\lambda_1^{n-1}\left(\alpha + \beta\left(\frac{\lambda_2}{\lambda_1}\right)^{n-1}\right)} = \lambda_1.$$

Finally, the sequence $(x_n)_{n\geq 1}$ is constant if $\alpha = 0$ or $\beta = 0$.

4. The sequence $(x_n)_{n\geq 1}$ is increasing and unbounded from above. Let us define

$$y_n = \frac{\ln x_n}{2^n}.$$

We have

$$y_{n+1} = \frac{\ln(x_n^2 + x_n)}{2^{n+1}} = y_n + \frac{\ln\left(1 + \frac{1}{x_n}\right)}{2^{n+1}} < y_n + \frac{1}{2^{n+1}x_n},$$

so

$$0 < y_{n+1} - y_n < \frac{1}{2^{n+1}x_n}.$$

Further,

$$\begin{aligned} 0 < y_{n+p} - y_n &< \frac{1}{2^{n+1}x_n} + \frac{1}{2^{n+2}x_{n+1}} + \ldots + \frac{1}{2^{n+p}x_{n+p-1}} \\ &< \frac{1}{x_n}\left(\frac{1}{2^{n+1}} + \frac{1}{2^{n+2}} + \ldots + \frac{1}{2^{n+p}}\right) \\ &= \frac{1}{x_n} \cdot \frac{1}{2^{n+1}} \cdot \frac{1 - \frac{1}{2^p}}{1 - \frac{1}{2}} < \frac{1}{2^n x_n}. \end{aligned}$$

This shows that sequence $(y_n)_{n\geq 1}$ is Cauchy, hence convergent; denote by λ its limit. If $\alpha = e^\lambda$, then from

$$0 < y_{n+p} - y_n < \frac{1}{2^n x_n},$$

it results by letting $p \to \infty$ that

$$0 \leq \ln\alpha - \frac{\ln x_n}{2^n} \leq \frac{1}{2^n x_n} \Leftrightarrow 0 \leq \ln\frac{\alpha^{2^n}}{x_n} \leq \frac{1}{x_n}.$$

Hence

$$\lim_{n\to\infty} \ln\frac{\alpha^{2^n}}{x_n} = 0$$

and finally,

$$\lim_{n\to\infty} \frac{\alpha^{2^n}}{x_n} = 1.$$

5. By the binomial theorem, it follows that

$$(2+\sqrt{3})^n + (2-\sqrt{3})^n = 2 \cdot \sum_{2k\leq n} \binom{n}{2k} \cdot 2^{n-2k} \cdot 3^k \in \mathbb{N},$$

hence, the numbers in the problem, a_n, are given by

$$a_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n - 1.$$

Now, the numbers $x_{1,2} = 2\pm\sqrt{3}$ are the roots of the quadratic polynomial

$$x^2 - 4x + 1.$$

The sequence $(s_n)_{n\geq 1}$ defined by $s_n = x_1^n + x_2^n$ satisfies the recurrence relation $s_{n+2} - 4s_{n+1} + s_n = 0$. Finally, $a_n = s_n - 1$, so

$$a_{n+2} = 4a_{n+1} - a_n - 2.$$

6. (RoMOP) We will prove that $\alpha = k + \sqrt{k^2-k}$ has the desired property. Let $\beta = k - \sqrt{k^2-k}$. As in the previous problem,

$$x_n = \alpha^n + \beta^n = [\alpha^n] + 1,$$

for all $n \geq 1$; also x_n has the property that

$$x_{n+2} - 2kx_{n+1} + kx_n = 0,$$

so, x_n is always a multiple of k, which shows that α has the desired property.

7. (RoMOP) The most typical way to solve this kind of problem is to consider for each x, the sequence $(x_n)_{n\geq 0}$ defined by

$$x_0 = x \quad \text{and} \quad x_{n+1} = f(x_n).$$

This sequence has the property that

$$x_{n+2} + ax_{n+1} = b(a+b)x_n.$$

The corresponding quadratic polynomial

$$x^2 + ax - b(a+b)$$

has the roots b and $-a-b$. Therefore, there are $\alpha, \beta \in \mathbb{R}$ such that

$$x_n = \alpha b^n + \beta(-a-b)^n = \alpha b^n + (-1)^n\beta(a+b)^n,$$

for all n. Since $x_n \geq 0$, it follows that

$$\alpha b^n \geq (-1)^{n+1}\beta(a+b)^n,$$

for all n. From here, it is not hard at all to deduce that $\beta = 0$, hence $x_n = \alpha b^n$, so, in particular, $x_1 = bx_0$, which actually means that $f(x) = bx$. This happens for all x, so $f(x) = bx$ is the only solution.

There is, however, a more elegant way to solve the problem without using sequences. Let

$$\alpha = \inf_{x>0} \frac{f(x)}{x} \text{ and } \beta = \sup_{x>0} \frac{f(x)}{x}.$$

Since $af(x) \le b(a+b)x$ for all x, $\beta \in \mathbb{R}$, on one hand,

$$b(a+b)x = f(f(x)) + af(x) \le \beta f(x) + af(x),$$

so

$$\frac{f(x)}{x} \ge \frac{b(a+b)}{a+\beta}, \forall x > 0 \Rightarrow \alpha \ge \frac{b(a+b)}{a+\beta} \tag{1}$$

while

$$b(a+b)x = f(f(x)) + af(x) \ge \alpha f(x) + af(x),$$

so

$$\frac{f(x)}{x} \le \frac{b(a+b)}{a+\alpha}, \forall x > 0 \Rightarrow \beta \le \frac{b(a+b)}{a+\alpha} \tag{2}$$

By (1) and (2) we easily deduce that $\alpha = \beta = b$, so $f(x) = bx$ for all $x \in \mathbb{R}$.

8. We have

$$\begin{aligned} a_n &= f_n^2 = (f_{n-1} + f_{n-2})^2 = f_{n-1}^2 + f_{n-2}^2 + 2f_{n-1}f_{n-2} \\ &= a_{n-1} + a_{n-2} + \frac{(f_{n-1} + f_{n-2})^2 - (f_{n-1} - f_{n-2})^2}{2} \\ &= a_{n-1} + a_{n-2} + \frac{f_n^2 - f_{n-3}^2}{2} = a_{n-1} + a_{n-2} + \frac{a_n - a_{n-3}}{2}, \end{aligned}$$

so

$$a_n = 2a_{n-1} + 2a_{n-2} - a_{n-3}.$$

9. The general term of the sum can be equivalently written as

$$\frac{1}{f_k f_{k+2}} = \frac{f_{k+1}}{f_k f_{k+1} f_{k+2}} = \frac{f_{k+2} - f_k}{f_k f_{k+1} f_{k+2}} = \frac{1}{f_k f_{k+1}} - \frac{1}{f_{k+1} f_{k+2}},$$

so

$$a_n = \sum_{k=1}^{n} \left(\frac{1}{f_k f_{k+1}} - \frac{1}{f_{k+1} f_{k+2}} \right) = \frac{1}{f_1 f_2} - \frac{1}{f_{n+1} f_{n+2}} = 1 - \frac{1}{f_{n+1} f_{n+2}},$$

hence the conclusion follows.

10. The sequence $(a_n)_{n\geq 1}$ satisfies a recurrence relation with the associated equation

$$3\lambda^3 - \lambda^2 - \lambda - 1 = 0.$$

The roots are

$$\lambda_1 = 1, \lambda_{2,3} = \frac{-1 \pm i\sqrt{2}}{3}$$

Using trigonometric form,

$$\lambda_{2,3} = \frac{1}{\sqrt{3}}(\cos\alpha \pm i\sin\alpha)$$

where $\alpha \in (\pi/2, \pi)$ is defined by $\cos\alpha = -\frac{1}{\sqrt{3}}$. The general term of the sequence $(a_n)_{n\geq 1}$ is

$$a_n = c_1 + \frac{1}{\sqrt{3^n}}(c_2\cos n\alpha + c_3\sin n\alpha),$$

so $(a_n)_{n\geq 1}$ converges to c_1. The coefficients c_1, c_2, c_3 can be calculated from the relations

$$\begin{cases} c_1 - \dfrac{1}{3}c_2 + \dfrac{\sqrt{2}}{3}c_3 = a \\ c_1 - \dfrac{1}{9}c_2 - \dfrac{2\sqrt{2}}{9}c_3 = b \\ c_1 + \dfrac{5}{27}c_2 + \dfrac{\sqrt{2}}{27}c_3 = c \end{cases}.$$

It follows that

$$c_1 = \frac{a + 2b + 3c}{6}.$$

11. (Danube International Competition 2005) Let

$$S_n = \sum_{k\geq 0}\binom{n}{2k+1}2005^k \text{ and } T_n = \sum_{k\geq 0}\binom{n}{2k}2005^k.$$

Then,

$$\left(1 \pm \sqrt{2005}\right)^n = T_n \pm S_n\sqrt{2005} \Rightarrow S_n = \frac{\left(1+\sqrt{2005}\right)^n - \left(1-\sqrt{2005}\right)^n}{\sqrt{2005}}.$$

Since $1 \pm \sqrt{2005}$ are the roots of $x^2 - 2x - 2004$, we have

$$S_{n+2} = 2S_{n+1} + 2004S_n,$$

from which the conclusion follows easily by induction.

12. (Romanian IMO TST 2006) We have to prove that

$$25 \leq x_{625} < 25 + \frac{1}{25}.$$

Squaring the given relation, we get

$$x_{n+1}^2 = x_n^2 + \frac{1}{4x_n^2} + 1 \Rightarrow x_{n+1}^2 - x_n^2 = 1 + \frac{1}{4x_n^2}.$$

It is clear that $x_n^2 \geq n$ (by induction). Therefore, the LHS of the inequality is already proved. For the RHS, we have

$$\begin{aligned} x_{625}^2 &= 1 + \sum_{k=1}^{624} \left(x_{k+1}^2 - x_k^2\right) = 625 + \frac{1}{4}\sum_{k=1}^{624} \frac{1}{x_k^2} \leq 625 + \frac{1}{4}\sum_{k=1}^{624} \frac{1}{k} \\ &\leq 625 + \frac{\ln 625}{4} = 625 + \frac{4\ln 5}{4} < 627 \\ &\Rightarrow x_{625} < 25 + \frac{1}{25}. \end{aligned}$$

13. Fix $m \in \mathbb{N}$. For all $n \in \mathbb{N}$, let

$$a_n = f^{n+1}(m) - f^n(m) - 667,$$

where the power denotes the number of times f is composed with itself. It is clear that

$$a_{n+1} + 2a_n \in \{0, 1\}$$

for all n. If $a_0 > 0$, a_{2n} tends to $+\infty$, which means that $a_{2n} + a_{2n+1}$ tends to $-\infty$, which finally means that the sequence $f^{2n+1}(m)$ is strictly decreasing from some rank, a contradiction. Analogously, we get a contradiction for $a_0 < 0$. Hence $a_0 = 0$, i.e., $f(m) = m + 667$. Hence $f(n) = n + 667$ is the only solution.

14. The associated equation of the recurrence is

$$\lambda^3 - \lambda - 1 = 0.$$

If we denote by $\lambda_1, \lambda_2, \lambda_3$ its roots, then, by Viète, $\lambda_1 + \lambda_2 + \lambda_3 = 0$. It is not hard to prove that

$$a_n = \lambda_1^n + \lambda_2^n + \lambda_3^n,$$

for all nonnegative integers n. For every prime number p, we have

$$\lambda_1^p + \lambda_2^p + \lambda_3^p \equiv (\lambda_1 + \lambda_2 + \lambda_3)^p \equiv 0 (\mathrm{mod}\, p),$$

so p divides a_p.

15. (IMO Shortlist 2004) We would like to find some a and b such that $\gcd(b, m) = 1$ and
$$x_n \equiv b^n \pmod{m}$$
for all n. For this, it is natural to take $a = 1$. Now, if we find some b such that
$$1 + b \equiv b^2 \pmod{m},$$
we are done. But this is not hard at all. We can take, for example, $b = 2k^2 + k - 2$. The solution is complete.

16. The equalities that define the sequence $(u_n)_{n\geq 0}$ show that the identity
$$u_0 + u_1X + u_2X^2 + \cdots = (c - bX + aX^2)(\lambda_0 + \lambda_1X + \lambda_2X^2 + \cdots)$$
is valid in the ring of formal series with real coefficients. Since $c \neq 0$, the series $c - bX + aX^2$ is invertible, thus we can read this equality like
$$\lambda_0 + \lambda_1X + \lambda_2X^2 + \cdots = (c - bX + aX^2)^{-1}(u_0 + u_1X + u_2X^2 + \cdots)$$
as well. But we can calculate the inverse of $c - bX + aX^2$ using its factorization
$$c - bX + aX^2 = a(r - X)(s - X)$$
(where r and s are the roots of the equation $ax^2 - bx + c = 0$) and the formula
$$(p - X)^{-1} = \frac{1}{p} + \frac{1}{p^2}X + \frac{1}{p^3}X^2 + \cdots = \sum_{n\geq 0} \frac{1}{p^{n+1}}X^n,$$
which is easy to check. We thus obtain the inverse of $c - bX + aX^2$:
$$\begin{aligned}(c - bX + aX^2)^{-1} &= \frac{1}{a}(r - X)^{-1}(s - X)^{-1}\\ &= \frac{1}{a}\left(\sum_{n\geq 0}\frac{1}{r^{n+1}}X^n\right)\left(\sum_{n\geq 0}\frac{1}{s^{n+1}}X^n\right),\end{aligned}$$
yielding
$$\sum_{n\geq 0}\lambda_nX^n = \frac{1}{a}\left(\sum_{n\geq 0}\frac{1}{r^{n+1}}X^n\right)\left(\sum_{n\geq 0}\frac{1}{s^{n+1}}X^n\right)\left(\sum_{n\geq 0}u_nX^n\right).$$
This equality for formal power series gives
$$\lambda_n = \sum_{i+j+k=n}\frac{u_k}{ar^{i+1}s^{j+1}}$$

for their coefficients (the sum being extended over all nonnegative integers i, j, and k that sum to n); that is, it provides an expression of each term of the sequence $(\lambda_n)_{n\geq 0}$ as a linear combination of some terms of the sequence $(u_n)_{n\geq 0}$. (Basically, we were given a second order, linear but nonhomogeneous, recurrence for the sequence $(\lambda_n)_{n\geq 0}$, and we solved it, finding out λ_n in terms of the u_ns.) If we remember that r and s are the roots of the equation $ax^2-bx+c=0$ and that a, b, c, and b^2-4ac are all positive, we see that r and s are positive real numbers. But this shows that the coefficients of the mentioned linear combination are positive as well, and the implication $u_n>0,\ \forall n\geq 0 \Rightarrow \lambda_n>0,\ \forall n\geq 0$ is now as clear as it can be.

This is problem 11445 proposed by H. A. ShahAli in *The American Mathematical Monthly.*

17. We prove the inequalities from part (a) by inducting on n. Since they are obviously true for $n=1$, assume that, for some n, we have $\sqrt{n}\leq u_n<\sqrt{n}+1$, and let us prove $\sqrt{n+1}\leq u_{n+1}<\sqrt{n+1}+1$. To this end, observe that

$$u_{n+1}=1+\frac{n}{u_n}\leq 1+\frac{n}{\sqrt{n}}=1+\sqrt{n}<1+\sqrt{n+1},$$

and

$$u_{n+1}=1+\frac{n}{u_n}>1+\frac{n}{\sqrt{n}+1}>1+\frac{n}{\sqrt{n+1}+1}=\sqrt{n+1}.$$

Note that the first inequality is actually strict if $n\geq 2$, and that both inequalities together yield $u_n\sim\sqrt{n}$ for $n\to\infty$ (that is, $\lim\limits_{n\to\infty}u_n/\sqrt{n}=1$).

Part a) is problem A proposed by John Scholes in *Nieuw Archief voor Wiskunde*, 1/2007.

b) The reader will easily see from the recurrence relation written in the form

$$u_{n+1}-\sqrt{n+1}+\frac{\sqrt{n}}{u_n}(u_n-\sqrt{n})=1-\frac{1}{\sqrt{n+1}+\sqrt{n}}$$

that, if the limit of $(u_n-\sqrt{n})_{n\geq 1}$ does exist, then it must be 1/2. However, proving the existence of this limit, for instance, by showing the monotonicity of the sequence seems pretty hard (*if* the monotonicity holds...). Thus we will try the same method, namely to use some inequalities — and we want them to be sharper than those from the problem statement (that barely demonstrate the boundedness of the sequence with general term $u_n - \sqrt{n}$). More precisely, we prove further that

$$\frac{1+\sqrt{4n-3}}{2} \leq u_n \leq \frac{1+\sqrt{4n+1}}{2}$$

for every positive integer n. We use again induction on n, and after verifying for $n = 1$ (the reader is kindly invited to do it), we assume the claimed inequalities to be true and show that

$$\frac{1+\sqrt{4n+1}}{2} \leq u_{n+1} \leq \frac{1+\sqrt{4n+5}}{2}$$

also hold. And indeed, we have:

$$u_{n+1} = 1 + \frac{n}{u_n} \geq 1 + \frac{2n}{1+\sqrt{4n+1}} = \frac{1+\sqrt{4n+1}}{2},$$

and

$$u_{n+1} = 1 + \frac{n}{u_n} \leq 1 + \frac{2n}{1+\sqrt{4n-3}} \leq 1 + \frac{-1+\sqrt{4n+5}}{2} = \frac{1+\sqrt{4n+5}}{2}.$$

The last inequality still needs explanation. It is equivalent to

$$4n \leq (\sqrt{4n+5}-1)(\sqrt{4n-3}+1),$$

and, after some calculations, to

$$(\sqrt{4n+5}-\sqrt{4n-3})^2 \leq 2(\sqrt{4n+5}-\sqrt{4n-3}).$$

Finally, this inequality is true because $\sqrt{4n+5}-\sqrt{4n-3} > 0$, and

$$\sqrt{4n+5}-\sqrt{4n-3} = \frac{8}{\sqrt{4n+5}+\sqrt{4n-3}} \leq \frac{8}{3+1} = 2.$$

Thus our stronger inequalities are proven. For the second part of the problem, just rewrite the inequalities in the form

$$\frac{1}{2} - \frac{3}{2(\sqrt{4n-3}+2\sqrt{n})} \leq u_n - \sqrt{n} \leq \frac{1}{2} + \frac{1}{2(\sqrt{4n+1}+2\sqrt{n})}$$

then let n go to infinity, in order to obtain $\lim_{n\to\infty}(u_n - \sqrt{n}) = 1/2$, as we guessed from the beginning.

Chapter 12

Sequences Given by Implicit Relations

In this chapter we give a method to find the convergence speed of a sequence given by an implicit relation, using the differentiability theorem of the inverse function.

Consider a sequence $(a_n)_{n\in\mathbb{N}}$ of real numbers and a function $f : \mathbb{R} \to \mathbb{R}$. We will study the properties of a sequence $(x_n)_{n\in\mathbb{N}}$ given by the following implicit relation:

$$f(x_n) = a_n, \tag{1}$$

for all $n \in \mathbb{N}$, where $x_0 \in \mathbb{R}$ is given. The next theoretical results show us the way to compute the limit of the sequence $(x_n)_{n\in\mathbb{N}}$ and then the convergence speed of $(x_n)_{n\in\mathbb{N}}$ to its limit. Note that almost every time, the sequence $(x_n)_{n\in\mathbb{N}}$ cannot be obtained explicitly, even if the function f is bijective.

Let $I, J \subseteq \mathbb{R}$ be two intervals. We prove the following:

Proposition. *Assume that the following conditions hold for the bijective function f:*

(i) the function $f : I \to J$ is continuous and bijective.

(ii) the sequence $(a_n)_{n\in\mathbb{N}}$ is convergent to $a \in \mathbb{R}$.

Then the sequence $(x_n)_{n\in\mathbb{N}}$ is convergent to $l = f^{-1}(a)$.

Proof. Indeed, the relation (1) can be equivalently written as

$$x_n = f^{-1}(a_n).$$

According to the continuity theorem of the inverse function, it follows that

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} f^{-1}(a_n) = f^{-1}(a).$$

Proposition. *Assume that the following conditions hold :*

(j) the function $f : I \to J$ *is differentiable and its derivative* f' *is continuous.*

(jj) the sequence $(a_n)_{n\in\mathbb{N}}$ *is convergent to* $a \in \mathbb{R}$.

Denote: $a = \lim\limits_{n\to\infty} a_n$ *and* $l = f^{-1}(a) = \lim\limits_{n\to\infty} x_n$. *If* $f'(l) \neq 0$, *then:*

$$\lim_{n\to\infty} \frac{x_n - l}{a_n - a} = \frac{1}{f'(l)}.$$

Proof. We have

$$\lim_{n\to\infty} \frac{x_n - l}{a_n - a} = \lim_{n\to\infty} \frac{f^{-1}(a_n) - f^{-1}(a)}{a_n - a} = \lim_{x\to a} \frac{f^{-1}(x) - f^{-1}(a)}{x - a} = (f^{-1})'(a).$$

Using the differentiability theorem of the inverse function, we obtain:

$$(f^{-1})'(a) = \frac{1}{f'(f^{-1}(a))} = \frac{1}{f'(l)},$$

so the conclusion is true.

Let us see now some applications of these results.

Problem. Let $(x_n)_{n\in\mathbb{N}}$ be a sequence of real numbers such that

$$x_n + \ln x_n = 1 + \frac{1}{n},$$

for all integers $n \geq 1$. Prove that:

a) $\lim\limits_{n\to\infty} x_n = 1$;

b) $\lim\limits_{n\to\infty} n(x_n - 1) = \frac{1}{2}$.

Solution. Let us consider the function $f : (0, \infty) \to \mathbb{R}$, given by

$$f(x) = x + \ln x.$$

We have

$$f'(x) = 1 + \frac{1}{x} > 0,$$

so f is increasing. But f is also continuous and

$$\lim_{x\searrow 0} f(x) = -\infty \quad , \quad \lim_{x\to\infty} f(x) = \infty,$$

so f is surjective. It follows that f is bijective. The given relation can be equivalently written as

$$f(x_n) = 1 + \frac{1}{n} \Rightarrow x_n = f^{-1}\left(1 + \frac{1}{n}\right).$$

We have

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} f^{-1}\left(1+\frac{1}{n}\right) = f^{-1}(1) = 1.$$

Further,

$$\begin{aligned}\lim_{n\to\infty} n(x_n-1) &= \lim_{n\to\infty} \frac{x_n-1}{\frac{1}{n}} = \lim_{n\to\infty} \frac{f^{-1}\left(1+\frac{1}{n}\right)-f^{-1}(1)}{\left(1+\frac{1}{n}\right)-1} \\ &= \left(f^{-1}\right)'(1) = \frac{1}{f'(1)} = \frac{1}{2}.\end{aligned}$$

Problem. Let $f : [a,b] \to \mathbb{R}$ be a continuously differentiable function with $f'(x) \neq 0$ for all x. Prove that:

a) for every $x \in (a,b]$, there exists a unique $c_x \in [a,x]$ such that

$$\int_a^x f(t)\,dt = f(c_x)(x-a).$$

b) $\lim\limits_{x\searrow a} \dfrac{c_x-a}{x-a} = \dfrac{1}{2}$.

Solution I. The existence of c_x follows from the *Leibniz-Newton* theorem and the uniqueness follows from the injectivity of f (the latter being a consequence of Rolle's theorem and of the hypothesis about the non-vanishing derivative). If

$$\int_a^x f(t)\,dt = f(c_x)(x-a) = f(\gamma_x)(x-a),$$

then $f(c_x) = f(\gamma_x)$, and consequently, $c_x = \gamma_x$. Now, using the differentiability theorem of the inverse function, then l'Hospital's rule, we obtain

$$\lim_{x\searrow a} \frac{c_x-a}{x-a} = \lim_{x\searrow a} \frac{f^{-1}\left(\dfrac{1}{x-a}\displaystyle\int_a^x f(t)\,dt\right)-a}{x-a}$$

$$= \lim_{x\searrow a}\left(\frac{f^{-1}\left(\dfrac{1}{x-a}\displaystyle\int_a^x f(t)\,dt\right)-f^{-1}(f(a))}{\dfrac{1}{x-a}\displaystyle\int_a^x f(t)\,dt-f(a)}\cdot\frac{\dfrac{1}{x-a}\displaystyle\int_a^x f(t)\,dt-f(a)}{x-a}\right)$$

$$= \lim_{x\searrow a}\frac{f^{-1}\left(\dfrac{1}{x-a}\displaystyle\int_a^x f(t)\,dt\right)-f^{-1}(f(a))}{\dfrac{1}{x-a}\displaystyle\int_a^x f(t)\,dt-f(a)}\cdot\lim_{x\searrow a}\frac{\dfrac{1}{x-a}\displaystyle\int_a^x f(t)\,dt-f(a)}{x-a}$$

$$= \left(f^{-1}\right)'(f(a)) \cdot \lim_{x \searrow a} \frac{\displaystyle\int_a^x f(t)\,dt - (x-a)f(a)}{(x-a)^2}$$

$$= \frac{1}{f'(a)} \cdot \lim_{x \searrow a} \frac{f(x)-f(a)}{2(x-a)} = \frac{1}{f'(a)} \cdot \frac{f'(a)}{2} = \frac{1}{2}.$$

Solution II. We have, by l'Hospital's rule, the fundamental theorem of calculus, and the definition of the derivative,

$$\lim_{x \searrow a} \frac{\displaystyle\int_a^x f(t)\,dt - f(a)(x-a)}{(x-a)^2} = \lim_{x \searrow a} \frac{f(x)-f(a)}{2(x-a)} = \frac{1}{2}f'(a),$$

hence, by replacing here $\int_a^x f(t)\,dt$ with $(x-a)f(c_x)$, we get

$$\lim_{x \searrow a} \frac{f(c_x)-f(a)}{x-a} = \frac{1}{2}f'(a).$$

On the other hand, because $c_x \in [a,x]$ implies $c_x \to a$ when $x \to a$, we have

$$\lim_{x \searrow a} \frac{f(c_x)-f(a)}{c_x-a} = f'(a).$$

In conclusion,

$$\lim_{x \searrow a} \frac{c_x-a}{x-a} = \lim_{x \searrow a} \frac{\dfrac{f(c_x)-f(a)}{x-a}}{\dfrac{f(c_x)-f(a)}{c_x-a}} = \frac{1}{2}.$$

Let us discuss some other problems, which are more challenging because they do not follow directly from the previous propositions. Before doing that, let us mention some standard notation. If $(x_n)_{n\ge1}$ and $(y_n)_{n\ge1}$ are two sequences such that $y_n \neq 0$ for all sufficiently large n, we write $x_n \sim y_n$ if $\lim\limits_{n\to\infty} \frac{x_n}{y_n} = 1$. If $y_n > 0$ for sufficiently large n, we write $x_n = o(y_n)$ if $\lim\limits_{n\to\infty} \frac{x_n}{y_n} = 0$ and $x_n = O(y_n)$ if $\left(\frac{x_n}{y_n}\right)_{n\ge1}$ is bounded.

Problem. Let $a > 0$ and let x_n be the unique solution of the equation $x \sin x = a \cos x$ lying in $\left(n\pi, n\pi + \frac{\pi}{2}\right)$. Prove that

$$x_n = n\pi + \frac{a}{n\pi} - \frac{a^2(a+3)}{3\pi^3 n^3} + O\left(\frac{1}{n^3}\right).$$

Solution. Let us prove first that x_n does exist, that is, the function

$$f(x) = x \sin x - a \cos x$$

has a unique zero in any interval $\left(n\pi, n\pi + \frac{\pi}{2}\right)$. Observe that on such an interval, $\sin x$ and $\cos x$ have the same sign, and since

$$f'(x) = x\cos x + (1+a)\sin x,$$

f' is strictly monotone on $I_n = \left(n\pi, n\pi + \frac{\pi}{2}\right)$. Note that

$$f(n\pi)f\left(n\pi + \frac{\pi}{2}\right) = -a\left(\frac{\pi}{2} + n\pi\right) < 0,$$

showing the existence and uniqueness of x_n.
Clearly, $x_n \sim n\pi$. Let $y_n = x_n - n\pi$. Then a simple computation shows that

$$\tan y_n = \frac{a}{n\pi + y_n} \Rightarrow y_n = \arctan\frac{a}{n\pi + y_n} \sim \frac{a}{n\pi}$$

because y_n is bounded and $\arctan x \sim x$ when $x \to 0$, i.e., $\lim\limits_{x\to 0}\frac{\arctan x}{x} = 1$.
Finally, let

$$z_n = y_n - \frac{a}{n\pi}.$$

From the previous step, $z_n = O\left(\frac{1}{n}\right)$, and the relation

$$y_n = \arctan\frac{a}{n\pi + y_n}$$

implies

$$z_n + \frac{a}{n\pi} = \arctan\frac{a}{n\pi + \frac{a}{n\pi} + O\left(\frac{1}{n}\right)}.$$

Observe that

$$\frac{a}{n\pi + \frac{a}{n\pi} + O\left(\frac{1}{n}\right)} = \frac{a}{n\pi} - \frac{a^2}{n^3\pi^3} + O\left(\frac{1}{n^3}\right)$$

and also that $\frac{\arctan x - x}{x^3}$ tends to $-\frac{1}{3}$ as $x \to 0$, yielding

$$\arctan x = x - \frac{x^3}{3} + o(x^3) = x - \frac{x^3}{3} + O(x^3).$$

Therefore

$$z_n + \frac{a}{n\pi} = \frac{a}{n\pi} - \frac{a^2}{n^3\pi^3} - \frac{a^3}{3n^3\pi^3} + O\left(\frac{1}{n^3}\right),$$

and the conclusion is immediate.

Less technical, the next exercise is also not obvious. The use of symbols introduced before the previous exercise turns out to be very advantageous.

Problem. Prove that for any $n > 1$, the equation

$$\sqrt[n]{x+1} - \sqrt[n]{x} = \frac{1}{n}$$

has a unique solution $x_n \in (0, 1)$. Prove that $\lim\limits_{n\to\infty} x_n = \dfrac{1}{e-1}$.

Solution. Consider $f : (0, 1) \to \mathbb{R}$, $f(x) = \sqrt[n]{x+1} - \sqrt[n]{x}$. Because

$$f(x) = \frac{1}{\sqrt[n]{x^{n-1}} + \ldots + \sqrt[n]{(x+1)^{n-1}}},$$

f is decreasing. Also, $f(0) = 1$ and $f(1) = \sqrt[n]{2} - 1 < \dfrac{1}{n}$ by Bernoulli's inequality (or simply the binomial formula for $\left(1 + \dfrac{1}{n}\right)^n$). Thus x_n exists and is unique. Observe that

$$\sqrt[n]{x_n} = \sqrt[n]{1 + x_n} - \frac{1}{n} > 1 - \frac{1}{n} \Rightarrow x_n > \left(1 - \frac{1}{n}\right)^n.$$

The sequence $\left(1 - \dfrac{1}{n}\right)^n$ converges to $\dfrac{1}{e}$, thus there exists a constant $c > 0$ such that $x_n > c$ for all n.

Now, this observation implies that

$$\frac{1}{\sqrt[n]{x_n}} = \sqrt[n]{1 + \frac{1}{x_n}} - 1 = e^{\frac{1}{n}\ln\left(1+\frac{1}{x_n}\right)} - 1 \sim \frac{1}{n}\ln\left(1 + \frac{1}{x_n}\right)$$

and since $\lim\limits_{n\to\infty} \sqrt[n]{x_n} = 1$ (because $1 \geq \sqrt[n]{x_n} \geq \sqrt[n]{c}$), we deduce that

$$\frac{1}{n} \sim \frac{1}{n}\ln\left(1 + \frac{1}{x_n}\right) \Rightarrow \ln\left(1 + \frac{1}{x_n}\right) \sim 1 \Rightarrow \lim_{n\to\infty} x_n = \frac{1}{e-1}.$$

Finally, we present a very technical problem that involves studying zeros of Taylor polynomials associated to the exponential function.

Problem. Let a_n be the unique real solution of the equation

$$1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^{2n+1}}{(2n+1)!} = 0.$$

Prove that this definition makes sense and that $\lim\limits_{n\to\infty} \dfrac{a_n}{n}$ exists.

Solution. Let us define $f_n(x) = 1 + \frac{x}{1!} + \ldots + \frac{x^n}{n!}$. First, we prove by induction that f_{2n} takes only positive values and f_{2n+1} is an increasing bijection of $\mathbb{R}$. This is clear for $n = 0$, so assume that it holds for n. Observe that $f'_{2n+2} = f_{2n+1}$, so if a_n is the unique zero of f_{2n+1} (because f_{2n+1} is bijective by the inductive hypothesis) then f_{2n+2} has a minimum in a_n. However,

$$f_{2n+2}(a_n) = f_{2n+1}(a_n) + \frac{a_n^{2n+2}}{(2n+2)!} = \frac{a_n^{2n+2}}{(2n+2)!} > 0,$$

thus f_{2n+2} is positive on $\mathbb{R}$. On the other hand, $f'_{2n+3} = f_{2n+2}$, thus f_{2n+3} is increasing and since it has odd degree, it is a bijection of $\mathbb{R}$. This finishes the induction and the first step of the problem: a_n is well-defined.

The second step consists of proving that a_n decreases towards $-\infty$.

Observe that

$$f_{2n+3}(x) - f_{2n+2}(x) = \frac{x^{2n+2}}{(2n+3)!}(2n+3+x).$$

If we manage to prove that $a_n + 2n + 3 > 0$, it will follow that $f_{2n+3}(a_n) > 0$, thus $a_n \geq a_{n+1}$ because f_{2n+3} is increasing. But

$$f_{2n+3}(-2n-3) = f_{2n+1}(-2n-3) \leq f_{2n+1}(-2n-1),$$

thus by induction, $f_{2n+1}(-2n-1) \leq f_1(-1) = 0$ for all n, thus $a_n \geq -2n-1$ and clearly $a_n + 2n + 3 > 0$. This shows that a_n is decreasing. Suppose that $\lim\limits_{n\to\infty} a_n = l$ is finite. Then by monotony and the fact that f_{2n+1} is increasing, we obtain $f_{2n+1}(l) \leq 0$, $\forall\ n$. However, we know that $\lim\limits_{n\to\infty} f_n(l) = e^l$, thus $e^l \leq 0$, which is clearly absurd. Thus $\lim\limits_{n\to\infty} a_n = -\infty$.

Now, let us prove that $\frac{a_n}{n}$ converges. Using Taylor-Lagrange's formula, we obtain the existence of a $c_n \in (a_n, 0)$ such that

$$e^{a_n} - f_{2n+2}(a_n) = \frac{e^{c_n}}{(2n+3)!}c_n^{2n+3} < 0,$$

thus

$$e^{a_n} \leq \frac{a_n^{2n+2}}{(2n+2)!} \Rightarrow a_n \leq (2n+2)\ln(-a_n) - \ln(2n+2)!.$$

The same argument shows that

$$e^{a_n} \geq \frac{a_n^{2n+2}}{(2n+3)!}(2n+3+a_n) \geq \frac{2a_n^{2n+2}}{(2n+3)!},$$

because we know that $a_n \geq -2n-1$ from the previous step.

Thus

$$\ln 2 + (2n+2)\ln(-a_n) - \ln(2n+3)! \leq a_n \leq (2n+2)\ln(-a_n) - \ln(2n+2)!.$$

Using Stirling's formula, $\ln n! = n \ln n - n + o(n)$, we deduce that

$$(2n+2)\left(1+\ln\frac{-a_n}{2n+2}\right) + o(n) \leq a_n \leq (2n+2)\left(1+\ln\frac{-a_n}{2n+2}\right) + o(n),$$

and therefore, $\lim\limits_{n\to\infty} b_n + \ln b_n = -1$, where $b_n = -\dfrac{a_n}{2n+2}$. The function $g(x) = x + \ln x$ being bijective, we deduce from the first proposition of the chapter that b_n converges to the unique solution ρ of the equation $x+\ln x = -1$. Thus $\lim\limits_{n\to\infty} \dfrac{a_n}{n} = -2\rho$.

Proposed Problems

1. Let $(x_n)_{n\geq 1}$ be a sequence of real numbers such that the sequence $(y_n)_{n\geq 1}$ given by the formula
$$y_n = x_n^3 + x_n$$
for all positive integers n, converges to 2. Prove that the sequence $(x_n)_{n\geq 1}$ converges to 1.

2. Let $(x_n)_{n\in\mathbb{N}} \subset (0,1)$ be a sequence given by the relation:
$$\tan x_n + \cos x_n = \sqrt[n]{n},$$
for all integers $n \geq 2$. Prove that:
   a) $\lim\limits_{n\to\infty} x_n = 0$;
   b) $\lim\limits_{n\to\infty} \dfrac{nx_n}{\ln n} = 1$.

3. Let $(x_n)_{n\in\mathbb{N}}$ be a sequence of real numbers such that
$$\frac{1}{x_n} + \arctan x_n = n,$$
for all nonnegative integers n. Prove that:
   a) $\lim\limits_{n\to\infty} x_n = 0$;
   b) $\lim\limits_{n\to\infty} nx_n = 1$.

4. Let $(x_n)_{n\geq 1}$ be a sequence of numbers greater than or equal to 1, given by the relation:
$$2^{x_n} - x_n = n(\sqrt[n]{e} - 1),$$
for all integers $n \geq 2$. Prove that:
   a) $\lim\limits_{n\to\infty} x_n = 1$;
   b) $\lim\limits_{n\to\infty} n(x_n - 1) = \dfrac{1}{2(\ln 4 - 1)}$.

5. Let $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ be sequences of nonzero real numbers satisfying:
$$\sin(a_n + b_n) = 2a_n + 3b_n,$$
for every nonnegative integer n. Prove that if $\lim\limits_{n\to\infty} a_n = 0$, then:
   a) $\lim\limits_{n\to\infty} b_n = 0$;
   b) $\lim\limits_{n\to\infty} \dfrac{a_n}{b_n} = -2$.

6. Prove that:
   a) for each real number x, there exists a unique real $y = y_x$ such that
$$\sin(x + y) = 2x + 3y.$$
   b) one can define a function $f : \mathbb{R} \to \mathbb{R}$, given by the relation $f(x) = y_x$, which is continuous. Compute $I = \displaystyle\int_0^{3\pi} f(x)\,dx$.

7. Let $f : [0, 1] \to (0, \infty)$ be continuous. Prove that:
   a) for any positive integer n, there exists a unique positive real number $a_n \in (0, 1)$ such that
$$\int_0^{a_n} f(t)\,dt = \frac{1}{n}\int_0^1 f(t)\,dt.$$
   b) $\lim\limits_{n\to\infty} a_n = 0$ and $\lim\limits_{n\to\infty} na_n = \dfrac{1}{f(0)}\displaystyle\int_0^1 f(t)\,dt$.

8. Prove that for every integer $n \geq 2$, there exists a solution of the equation $x^n = x + n$, denoted by a_n such that the sequence $(a_n)_{n\geq 2}$ converges to 1.

9. Prove that for every positive integer n, the equation
$$x^3 + nx - 1 = 0$$
has a solution $a_n \in [0, 1]$. Prove that the sequence $(a_n)_{n\geq 1}$ converges to zero and the sequence $(b_n)_{n\geq 1}$ given by the formula $b_n = na_n$ converges to 1.

10. Prove that for every integer $n \geq 3$, the equation

$$x^n - nx + 1 = 0$$

has a solution in $(0,1)$ and another solution greater than 1. If we denote by $a_n \in (0,1)$ and $b_n \in (1,\infty)$ those solutions, prove that the sequence $(a_n)_{n\geq 1}$ converges to zero and the sequence $(b_n)_{n\geq 1}$ converges to 1.

11. Let $(a_n)_{n\geq 1}$ be a sequence of distinct real numbers with the following property: for every $\varepsilon > 0$, there exists $\eta > 0$ such that $|a_{m+1} - a_{n+1}| < \varepsilon$ whenever m and n are positive integers such that $\varepsilon \leq |a_m - a_n| < \varepsilon + \eta$. Prove that $(a_n)_{n\geq 1}$ is convergent.

Solutions

1. Let us consider the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3 + x$. From the fact that $f'(x) = 3x^2 + 1 > 0$, it follows that f is strictly increasing and consequently injective. The function f is continuous with

$$\lim_{x\to-\infty} f(x) = -\infty, \quad \lim_{x\to\infty} f(x) = \infty,$$

so f is surjective. In conclusion, f is bijective. Then

$$y_n = x_n^3 + x_n \Leftrightarrow y_n = f(x_n)$$

and by applying f^{-1}, we obtain that

$$x_n = f^{-1}(y_n).$$

The function f^{-1} is continuous together with f. So, the hypothesis implies

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} f^{-1}(y_n) = f^{-1}(2).$$

Obviously, $f(1) = 2$, so $f^{-1}(2) = 1$. In conclusion, the sequence $(x_n)_{n\geq 1}$ converges to 1.

2. Let us consider the function $f : [0,1] \to [1, \tan 1 + \cos 1]$,

$$f(x) = \tan x + \cos x.$$

We have

$$f'(x) = \frac{1}{\cos^2 x} - \sin x > 0,$$

so f is increasing. Then

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} f^{-1}(\sqrt[n]{n}) = f^{-1}(1) = 0.$$

Further,

$$\begin{aligned}\lim_{n\to\infty}\frac{nx_n}{\ln x_n} &= \lim_{n\to\infty}\left(\frac{f^{-1}(\sqrt[n]{n})-f^{-1}(1)}{\sqrt[n]{n}-1}\cdot\frac{n}{\ln n}\cdot(\sqrt[n]{n}-1)\right)\\ &= (f^{-1})'(1)\cdot\lim_{n\to\infty}\frac{\sqrt[n]{n}-1}{\ln\sqrt[n]{n}} = (f^{-1})'(1)\\ &= \frac{1}{f'(0)} = 1.\end{aligned}$$

3. Let us define the function $f:(0,\infty)\to(\pi/2,\infty)$, by

$$f(x)=\frac{1}{x}+\arctan x.$$

We have

$$f'(x)=-\frac{1}{x^2}+\frac{1}{1+x^2}=\frac{-1}{x^2(1+x^2)}<0,$$

so f is decreasing. Moreover,

$$\lim_{n\to\infty}x_n=\lim_{n\to\infty}f^{-1}(n)=0,$$

because $\lim\limits_{x\to 0}f(x)=\infty$. Further, the given relation can be equivalently written as

$$\frac{1}{nx_n}+\frac{\arctan x_n}{n}=1. \tag{1}$$

The sequence $(x_n)_{n\geq 1}$ tends to zero, so we have

$$\lim_{n\to\infty}\frac{\arctan x_n}{n}=0.$$

Now we can easily derive from (1) that $\lim\limits_{n\to\infty}nx_n=1$.

4. Let us define the function $f:\mathbb{R}\to\mathbb{R}$ by $f(x)=2^x-x$. Clearly, $f(1)=1$ and f tends to ∞ as x tends to ∞. Also, $f'(x)>0$ if $x\geq 1$. Thus f establishes an increasing bijection between $[1,\infty)$ and $[1,\infty)$. Also, the inequality $e^x\geq x+1$ shows that $n(\sqrt[n]{e}-1)\geq 1$. We have

$$x_n=f^{-1}(n\left(\sqrt[n]{e}-1\right)).$$

With

$$\lim_{n\to\infty}n\left(\sqrt[n]{e}-1\right)=\lim_{n\to\infty}\frac{e^{\frac{1}{n}}-1}{\frac{1}{n}}=\lim_{x\to 0}\frac{e^x-1}{x}=1$$

and using the continuity of the function f^{-1}, it follows that

$$\lim_{n\to\infty}x_n=\lim_{n\to\infty}f^{-1}(n\left(\sqrt[n]{e}-1\right))=f^{-1}(1)=1.$$

Further,

$$\begin{aligned}\lim_{n\to\infty} n(x_n-1) &= \lim_{n\to\infty} \frac{f^{-1}(n(\sqrt[n]{e}-1))-f^{-1}(1)}{n(\sqrt[n]{e}-1)-1}\cdot\frac{n(\sqrt[n]{e}-1)-1}{\frac{1}{n}}\\ &= \lim_{n\to\infty} \frac{f^{-1}(n(\sqrt[n]{e}-1))-f^{-1}(1)}{n(\sqrt[n]{e}-1)-1}\cdot\lim_{n\to\infty}\frac{n(\sqrt[n]{e}-1)-1}{\frac{1}{n}}\\ &= (f^{-1})'(1)\cdot\lim_{n\to\infty} n\left(\frac{e^{1/n}-1}{1/n}-1\right)\\ &= \frac{1}{f'(1)}\cdot\lim_{x\to 0}\frac{1}{x}\left(\frac{e^x-1}{x}-1\right)\\ &= \frac{1}{\ln 4-1}\cdot\frac{1}{2}=\frac{1}{2(\ln 4-1)},\end{aligned}$$

where the last limit is calculated with *l'Hôpital's* rule:

$$\begin{aligned}\lim_{x\to 0}\frac{1}{x}\left(\frac{e^x-1}{x}-1\right) &= \lim_{x\to 0}\frac{e^x-1-x}{x^2}=\lim_{x\to 0}\frac{e^x-1}{2x}\\ &= \lim_{x\to 0}\frac{e^x}{2}=\frac{1}{2}.\end{aligned}$$

5. The sequence $(b_n)_{n\geq 0}$ is bounded together with $(a_n)_{n\geq 0}$. To prove this, let us assume that the sequence $(a_n)_{n\in\mathbb{N}}$ is bounded by M. Then from the given relation, we obtain

$$|b_n| = \left|\frac{\sin(a_n+b_n)-2a_n}{3}\right| \leq \frac{|\sin(a_n+b_n)|+2|a_n|}{3}\leq\frac{1+2M}{3}.$$

If $(b_n)_{n\geq 0}$ has two subsequences $(b_{k_n})_{n\geq 0}$, $(b_{p_n})_{n\geq 0}$ converging to l_1, respectively l_2, then from

$$\sin(a_{k_n}+b_{k_n})=2a_{k_n}+3b_{k_n},\quad \sin(a_{p_n}+b_{p_n})=2a_{p_n}+3b_{p_n},$$

we derive, by taking the limit as $n\to\infty$,

$$\sin l_1 = 3l_1\ ,\ \sin l_2 = 3l_2,$$

so $l_1=l_2=0$. For the second part, note that

$$\lim_{n\to\infty}\frac{\sin(a_n+b_n)}{a_n+b_n}=\lim_{x\to 0}\frac{\sin x}{x}=1,$$

so

$$1=\lim_{n\to\infty}\frac{2a_n+3b_n}{a_n+b_n}=\lim_{n\to\infty}\frac{2\frac{a_n}{b_n}+3}{\frac{a_n}{b_n}+1}.$$

It easily follows that $\lim\limits_{n\to\infty}\frac{a_n}{b_n}=-2$.

6. If $x + y = t$, then the condition becomes $2x + 3y = \sin t$. Now from the system

$$\begin{cases} x + y = t \\ 2x + 3y = \sin t, \end{cases}$$

we obtain $x = \phi(t)$, $y = \psi(t)$, where

$$\phi(t) = 3t - \sin t \ , \ \psi(t) = -2t + \sin t.$$

The function ϕ is continuous with

$$\lim_{t\to-\infty} \phi(t) = -\infty, \quad \lim_{t\to\infty} \phi(t) = \infty,$$

so ϕ is surjective. For injectivity, note that $\phi'(t) = 3 - \cos t > 0$. Thus the function ϕ is invertible, so $y = \psi(\phi^{-1}(x))$.

Further, with the change of variable $x = \phi(t)$, $t \in [0, \pi]$, we have

$$\begin{aligned} I &= \int_0^{3\pi} f(x)\,dx = \int_0^{3\pi} \psi(\phi^{-1}(x))\,dx = \int_0^{\pi} \psi(t)\phi'(t)\,dt \\ &= \int_0^{\pi} (-2t + \sin t)(3 - \cos t)\,dt = 6 - 3\pi^2. \end{aligned}$$

7. Let us define the continuous function $F : [0, 1] \to \mathbb{R}$ given by

$$F(x) = \int_0^x f(t)\,dt.$$

We have

$$F(0) < \frac{1}{n}\int_0^1 f(t)\,dt < F(1),$$

so the value

$$\frac{1}{n}\int_0^1 f(t)\ dt$$

is an intermediate value between $F(0)$ and $F(1)$. The function F is continuous, so

$$F(a_n) = \frac{1}{n}\int_0^1 f(t)\,dt,$$

for some $a_n \in (0, 1)$. Then

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} F^{-1}\left(\frac{1}{n}\int_0^1 f(t)\,dt\right) = F^{-1}(0) = 0.$$

Further,

$$\begin{aligned}\lim_{n\to\infty} na_n &= \lim_{n\to\infty}\left(\frac{F^{-1}\left(\frac{1}{n}\int_0^1 f(t)\,dt\right) - F^{-1}(0)}{\frac{1}{n}\int_0^1 f(t)\,dt - 0}\cdot\int_0^1 f(t)\,dt\right)\\
&= \int_0^1 f(t)\,dt\cdot\lim_{n\to\infty}\frac{F^{-1}\left(\frac{1}{n}\int_0^1 f(t)\,dt\right) - F^{-1}(0)}{\frac{1}{n}\int_0^1 f(t)\,dt - 0}\\
&= (F^{-1})'(0)\int_0^1 f(t)\,dt = \frac{1}{F'(0)}\int_0^1 f(t)\,dt\\
&= \frac{1}{f(0)}\int_0^1 f(t)\,dt.\end{aligned}$$

We can also use the mean value theorem. If $0 < c_n < a_n$ satisfies

$$\int_0^{a_n} f(t)\,dt = a_n f(c_n),$$

then

$$a_n f(c_n) = \frac{1}{n}\int_0^1 f(t)\,dt$$

$$\Rightarrow na_n = \frac{1}{f(c_n)}\int_0^1 f(t)\,dt \to \frac{1}{f(0)}\int_0^1 f(t)\,dt\,,\quad\text{as}\quad n\to\infty.$$

8. Let us consider the polynomial

$$P(x) = x^n - x - n.$$

Then $P(1) = -n < 0$ and $P(\sqrt[n]{2n}) = 2n - \sqrt[n]{2n} - n = n - \sqrt[n]{2n} \geq 0$. Using the continuity of P, there exists a real number $a_n \in (1, \sqrt[n]{2n}]$ such that $P(a_n) = 0$. Because $1 < a_n < \sqrt[n]{2n}$, the sequence $(a_n)_{n\geq 1}$ converges to 1.

9. Let us consider the polynomial function

$$P(x) = x^3 + nx - 1.$$

We have

$$P'(x) = 3x^2 + n > 0,$$

so P is increasing. Then $P(0) = -1 < 0$ and $P(1) = n \geq 1$, so there exists a unique real number $a_n \in [0,1]$ such that $P(a_n) = 0$. From the relation

$$a_n^3 + na_n - 1 = 0,$$

we deduce that

$$0 \leq a_n = \frac{1 - a_n^3}{n} \leq \frac{1}{n}.$$

Hence the sequence $(a_n)_{n\geq 1}$ converges to zero. Finally,

$$\lim_{n\to\infty} na_n = \lim_{n\to\infty} (1 - a_n^3) = 1.$$

10. Let us consider the polynomial function

$$P(x) = x^n - nx + 1.$$

Using the continuity of P and the fact that

$$P(0) = 1 > 0, \quad P(1) = 2 - n < 0,$$

we deduce that the polynomial P has a root $a_n \in (0,1)$. Then

$$P(1) < 0, \quad \lim_{x\to\infty} P(x) = \infty,$$

so there exists a real number $b_n \in (1, \infty)$ such that $P(b_n) = 0$. From the relation

$$a_n^n - na_n + 1 = 0,$$

it follows that

$$0 \leq a_n = \frac{a_n^n + 1}{n} \leq \frac{2}{n} \to 0,$$

so the sequence $(a_n)_{n\geq 1}$ converges to zero.
Then with the notation $b_n = 1 + c_n$, we obtain

$$n(1 + c_n) = (1 + c_n)^n - 1 > \left(1 + nc_n + \frac{n(n-1)}{2} \cdot c_n^2\right) - 1.$$

Hence

$$0 < c_n < \sqrt{\frac{2}{n-1}}.$$

Hence the sequence $(c_n)_{n\geq 1}$ converges to zero and consequently, the sequence $(b_n)_{n\geq 1}$ converges to 1.

11. Well, this is not quite about sequences defined by implicit relations, but it states the convergence of a sequence in an implicit way, so that's why it appears here. In both solutions that follow we will show that the given sequence is Cauchy (which can also be considered an implicit way of proving the convergence of a sequence).

    Solution I. We first note that the condition about $(a_n)_{n\geq 1}$ implies, with $\varepsilon = |a_m - a_n|$ (and it doesn't matter whatever η would be), that $|a_{m+1} - a_{n+1}| < |a_m - a_n|$ for all positive and distinct integers m and n. Thus, the sequence $(|a_{m+k} - a_{n+k}|)_{k\geq 0}$ is strictly decreasing and bounded below, hence convergent. With the limit of this sequence in place of ε, we immediately see that this limit is necessarily zero for every pair (m, n) of distinct positive integers.

    Suppose, by way of contradiction, that $(a_n)_{n\geq 1}$ is not a Cauchy sequence. In that case, we can find some $\alpha > 0$ such that for every positive integer N, there exist $m > n > N$ such that $|a_m - a_n| \geq \alpha$. Choose $\varepsilon > 0$ and the corresponding η (ensured by the hypothesis) such that $\varepsilon + \eta \leq \alpha$ (note that if an η is good, any smaller value is also convenient).

    Because $\lim\limits_{n\to\infty} |a_{n+1} - a_n| = 0$, we can find a positive integer N such that $|a_{n+1} - a_n| < \eta/4$ for all $n \geq N$. As we said, we can find $m > n > N$ such that $|a_m - a_n| \geq \alpha$, and further we fix our attention to these m and n.

    As noticed above, the sequence $(a_{m+k} - a_{n+k})_{k\geq 0}$ has limit 0, and we have $|a_m - a_n| \geq \alpha \geq \varepsilon + \eta$, hence there must be some $k \geq 1$ with the property

    $$|a_{m+k-1} - a_{n+k-1}| \geq \varepsilon + \eta > |a_{m+k} - a_{n+k}|.$$

    On the other hand, for every $s \geq 0$, we have

    $$\begin{aligned}|a_{m+s} - a_{n+s}| &\leq |a_{m+s} - a_{m+s+1}| + |a_{m+s+1} - a_{n+s+1}| + |a_{n+s+1} - a_{n+s}| \\ &< |a_{m+s+1} - a_{n+s+1}| + \frac{\eta}{2}.\end{aligned}$$

    In particular, this holds for $s = k - 1$:

    $$|a_{m+k-1} - a_{n+k-1}| - \frac{\eta}{2} < |a_{m+k} - a_{n+k}|,$$

    and, combining this with the above inequalities, we get

    $$\varepsilon < \varepsilon + \frac{\eta}{2} \leq |a_{m+k-1} - a_{n+k-1}| - \frac{\eta}{2} < |a_{m+k} - a_{n+k}| < \varepsilon + \eta.$$

    By hypothesis, these lead to $|a_{m+k+1} - a_{n+k+1}| < \varepsilon$.

However, we also must have

$$|a_{m+k+1} - a_{n+k+1}| > |a_{m+k} - a_{n+k}| - \frac{\eta}{2} > \varepsilon + \frac{\eta}{2} - \frac{\eta}{2} = \varepsilon,$$

and the contradiction thus obtained shows that our assumption is wrong, that is, $(a_n)_{n\geq 1}$ is Cauchy (therefore convergent).

Solution II. We use the same basic ideas, but with a different wording. As in the first solution, we prove that for every positive integer k, $(|a_{n+k} - a_n|)_{n\geq 1}$ is a strictly decreasing and convergent to zero sequence.

Consider an arbitrary positive ε and the corresponding η given by the hypothesis. Because we have

$$|a_{1+k} - a_1| > |a_{2+k} - a_2| > \cdots$$

and $\lim_{n\to\infty} |a_{n+k} - a_n| = 0$, there exists (for any natural $k \geq 1$) such a natural number n_k with the property

$$|a_{1+k} - a_1| > \cdots > |a_{n_k+k} - a_{n_k}| \geq \varepsilon > |a_{n_k+k+1} - a_{n_k+1}| > \cdots$$

(n_k is considered to be 0 if all terms of the sequence $(|a_{n+k} - a_n|)_{n\geq 1}$ are less than ε).

Let us suppose that the sequence $n_1, n_2, \ldots$ is unbounded. Remembering that $\lim_{n\to\infty} |a_{n+1} - a_n| = 0$, we can be sure of the existence of a natural number N having the property

$$|a_{n+1} - a_n| < \frac{\eta}{4}, \forall n > N$$

(for the η considered in the beginning). Because $(n_k)_{k\geq 1}$ is not bounded, there is k for which $n_k > N + 1$, therefore, by the triangle inequality (and those above),

$$\begin{aligned}|a_{n_k+k-1} - a_{n_k-1}| &\leq |a_{n_k+k} - a_{n_k+k-1}| + |a_{n_k+k+1} - a_{n_k+k}| \\ &\quad + |a_{n_k+k+1} - a_{n_k+1}| + |a_{n_k+1} - a_{n_k}| + |a_{n_k} - a_{n_k-1}| \\ &< \frac{\eta}{4} + \frac{\eta}{4} + \varepsilon + \frac{\eta}{4} + \frac{\eta}{4} = \varepsilon + \eta,\end{aligned}$$

hence our assumption leads to the conclusion

$$\varepsilon \leq |a_{n_k+k} - a_{n_k}| < |a_{n_k+k-1} - a_{n_k-1}| < \varepsilon + \eta,$$

which evidently contradicts the hypothesis. This shows our assumption to be false, that is, the sequence $(n_k)_{k\geq 1}$ is bounded. But if M is a natural number greater than all numbers n_k, it is clear that for any $n > M$ and any $k \geq 1$, we have

$$|a_{n+k} - a_n| < \varepsilon;$$

since ε is an arbitrary positive number, this means that $(a_n)_{n\geq 1}$ is a Cauchy sequence, therefore a convergent one.

This is problem 11207 proposed by Michael W. Botsko in *The American Mathematical Monthly*, 2/2006. The first solution, by Robert B. Israel, appeared in the same magazine, 10/2007.

Chapter 13

Matrices Associated to Second Order Recurrences

We give here two matrix relations associated to second order recurrences. In some cases, interesting properties of sequences given by second order recurrences can be established using these relations. Note that sometimes the expression of the general term cannot be used. Finally, three examples from mathematical competitions are given.

Let p and q be real numbers and consider a sequence of real numbers $(a_n)_{n\geq 1}$. Note that the following matrix equality holds:

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix} = \begin{pmatrix} a_{n+1} & -pa_{n+1} - qa_n \\ a_{n+3} & -pa_{n+3} - qa_{n+2} \end{pmatrix}, \tag{1}$$

for all positive integers n. The form of the elements from the second column of the matrix in the right-hand side shows us the connection of relation (1) with sequences given by second order relations. More precisely, we have the following:

Theorem. *Let p, q be real numbers and let $(a_n)_{n\geq 1}$ be a sequence given by the recurrence*

$$a_{n+2} + pa_{n+1} + qa_n = 0, \quad n \geq 1.$$

with $a_1, a_2 \in \mathbb{R}$. Then

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix} = \begin{pmatrix} a_{n+1} & a_{n+2} \\ a_{n+3} & a_{n+4} \end{pmatrix}, \tag{2}$$

for all positive integers n. Moreover,

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}^{n-1}, \tag{3}$$

for all positive integers n.

The relation (2) follows from (1), using the equalities

$$-pa_{n+2} - qa_{n+1} = a_{n+3} \quad \text{and} \quad -pa_{n+3} - qa_{n+2} = a_{n+4}.$$

The relation (3) can be easily proved by induction. It is true for $n = 1$ and if we assume that it is true for n, then it follows from (2):

$$\begin{pmatrix} a_{n+1} & a_{n+2} \\ a_{n+3} & a_{n+4} \end{pmatrix} = \begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}^{n-1} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}^{n}.$$

Similarly, we have the following:

Theorem. *Let p, q be real numbers and let $(a_n)_{n\geq 1}$ be a sequence given by the recurrence*

$$a_{n+2} + pa_{n+1} + qa_n = 0, \quad n \geq 1.$$

with $a_1, a_2 \in \mathbb{R}$. Then

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+1} & a_{n+2} \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix} = \begin{pmatrix} a_{n+1} & a_{n+2} \\ a_{n+2} & a_{n+3} \end{pmatrix} \tag{4}$$

for all positive integers n.Moreover,

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+1} & a_{n+2} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_3 \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}^{n-1}, \tag{5}$$

for all positive integers n.

Now we show how these theoretical results can be used in practical problems. We present a problem from the Bulgarian Mathematical Olympiad, 1997.

Problem. Let $\alpha \neq \beta$ be the roots of the quadratic equation $x^2+px+q = 0$. For each positive integer n, we put

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

a) Find all real numbers p and q for which

$$a_{n+1}a_{n+2} - a_na_{n+3} = (-1)^n,$$

for all positive integers n.

b) Prove that for these values for p and q, we have

$$a_n + a_{n+1} = a_{n+2},$$

for all positive integers n and a_n is even if 3 divides n.

Solution. a) The sequence $(a_n)_{n\geq 1}$ satisfies the second order recurrence

$$a_{n+2} + pa_{n+1} + qa_n = 0. \tag{6}$$

Indeed,

$$\begin{aligned} a_{n+2} + pa_{n+1} + qa_n &= \frac{\alpha^{n+2} - \beta^{n+2}}{\alpha - \beta} + p \cdot \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} + q \cdot \frac{\alpha^n - \beta^n}{\alpha - \beta} \\ &= \frac{1}{\alpha - \beta}\left[\alpha^n\left(\alpha^2 + p\alpha + q\right) - \beta^n\left(\beta^2 + p\beta + q\right)\right] = 0, \end{aligned}$$

because α and β are roots and the expressions from the brackets are zero. Now, for the sequence $(a_n)_{n\geq 1}$, we also have

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}^{n-1},$$

for all positive integers n. By taking the determinant, we deduce

$$\begin{vmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{vmatrix} = \begin{vmatrix} a_1 & a_2 \\ a_3 & a_4 \end{vmatrix} \cdot \begin{vmatrix} 0 & -q \\ 1 & -p \end{vmatrix}^{n-1}$$

or

$$a_n a_{n+3} - a_{n+1}a_{n+2} = (a_1a_4 - a_2a_3) \cdot q^{n-1}.$$

But $a_{n+1}a_{n+2} - a_na_{n+3} = (-1)^n$, so

$$(a_1a_4 - a_2a_3) \cdot q^{n-1} = (-1)^{n-1},$$

for all positive integers n. Thus, we impose the conditions

$$q = -1 \quad \text{and} \quad a_1a_4 - a_2a_3 = 1.$$

In order to determine p, we have

$$a_1a_4 - a_2a_3 = 1$$

$$\Rightarrow \frac{\alpha - \beta}{\alpha - \beta} \cdot \frac{\alpha^4 - \beta^4}{\alpha - \beta} - \frac{\alpha^2 - \beta^2}{\alpha - \beta} \cdot \frac{\alpha^3 - \beta^3}{\alpha - \beta} = 1$$

$$\Rightarrow (\alpha - \beta)\left(\alpha^4 - \beta^4\right) - \left(\alpha^2 - \beta^2\right)\left(\alpha^3 - \beta^3\right) = (\alpha - \beta)^2.$$

Dividing by $(\alpha - \beta)^2$, we obtain

$$(\alpha^3 + \alpha^2\beta + \alpha\beta^2 + \beta^3) - (\alpha + \beta)(\alpha^2 + \alpha\beta + \beta^2) = 1$$

or simply,

$$\alpha\beta(\alpha+\beta)=1.$$

According to Viète's relations, we have

$$\alpha\beta=q=-1$$

and so

$$p=-(\alpha+\beta)=-1.$$

Hence, $p=q=-1$.

b) With $p=q=-1$ we have

$$a_n+a_{n+1}=a_{n+2}.$$

Further, we use the equality

$$X_{n+1}=X_nA,$$

where

$$X_n=\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix}, \quad A=\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Now, from $X_{n+3}=X_nA^3$, we deduce

$$\begin{pmatrix} a_{n+3} & a_{n+4} \\ a_{n+5} & a_{n+6} \end{pmatrix}=\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$$

or

$$\begin{pmatrix} a_{n+3} & a_{n+4} \\ a_{n+5} & a_{n+6} \end{pmatrix}=\begin{pmatrix} a_n+2a_{n+1} & 2a_n+3a_{n+1} \\ a_{n+2}+2a_{n+3} & 2a_{n+2}+3a_{n+3} \end{pmatrix}.$$

By identifying the elements from the first row and first column, we obtain

$$a_{n+3}=a_n+2a_{n+1}$$

and by induction, a_n is even if n is divisible by 3.

Proposed Problems

1. a) Let $(a_n)_{n\geq 1}$ be a sequence of real numbers given by the following recurrence

$$a_{n+2}+pa_{n+1}+qa_n=0, \quad n\geq 1,$$

where p, q, a_1, $a_2\in\mathbb{R}$. Prove that if the expression

$$\frac{a_na_{n+3}-a_{n+1}a_{n+2}}{a_na_{n+2}-a_{n+1}^2}$$

is well defined (that is, its denominator is not zero) for all positive integers n, then it has a constant value, which does not depend on n.

b) Conversely, let $(a_n)_{n\geq 1}$ be a sequence of real numbers for which the expression

$$\frac{a_n a_{n+3} - a_{n+1}a_{n+2}}{a_n a_{n+2} - a_{n+1}^2}$$

is well defined for all positive integers n, and assume that it has a constant value, independent of n. Prove that the sequence $(a_n)_{n\geq 1}$ satisfies a second order recurrence.

2. Let $(a_n)_{n\geq 1}$ be a sequence with the property that for each integer $n \geq 2$,

$$a_{n+1} = pa_n + a_{n-1},$$

where p, a_1, and a_2 are given. Prove that:

a) there exists a real number λ such that for all $n \geq 1$,

$$a_n a_{n+3} - a_{n+1}a_{n+2} = (-1)^n \lambda.$$

b) there exists a real number μ such that for all $n \geq 1$,

$$a_n a_{n+2} - a_{n+1}^2 = (-1)^n \mu.$$

3. Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of nonzero real numbers such that

$$a_n^2 - a_{n-1}a_{n+1} = 1,$$

for all positive integers n. Prove that there exists a real number λ such that

$$a_{n+1} = \lambda a_n - a_{n-1},$$

for all $n \geq 1$.

4. For a sequence $(a_n)_{n\geq 1}$ of real numbers there exist matrices A, $B \in \mathcal{M}_2(\mathbb{R})$ such that

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} = A \cdot B^{n-1},$$

for all integers $n \geq 1$. Prove that the sequence $(a_n)_{n\geq 1}$ satisfies a second order recurrence.

5. Let $(a_n)_{n\geq 1}$ be a sequence of real numbers such that for every integer $n \geq 2$,
$$a_{n+1} = 2a_n + a_{n-1},$$
where a_1 and a_2 are given. Prove that the sum of every two consecutive terms of the sequence
$$x_n = a_n a_{n+1}, \quad n \geq 1$$
is a term of the sequence $(a_n)_{n\geq 1}$.

6. Let $(L_n)_{n\geq 0}$ be Lucas's sequence given for all $n \geq 2$ by
$$L_n = L_{n-1} + L_{n-2},$$
where $L_0 = 2$, $L_1 = 1$. Prove that for all integers $n \geq 2$,
a) $5L_{2n} = 2L_n^2 + L_{n+1}^2 + L_{n-1}^2$;
b) $5L_{2n+1} = L_{n+2}^2 + 2L_n L_{n-1}$.

7. Let $(F_n)_{n\geq 0}$ and $(L_n)_{n\geq 0}$ be Fibonacci's sequence, respectively Lucas's sequence, given by the recurrences
$$F_{n+2} = F_{n+1} + F_n, \; F_0 = 1, \; F_1 = 1$$
$$L_{n+2} = L_{n+1} + L_n, \; L_0 = 2, \; L_1 = 1.$$
Prove the matrix identity:
$$\begin{pmatrix} F_{2n} & F_{2n+1} \\ L_{2n} & L_{2n+1} \end{pmatrix} = \begin{pmatrix} F_{n-1} + F_{n+1} & -F_{n-1} \\ L_n + L_{n+1} & -L_{n-1} \end{pmatrix} \begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix}.$$

8. Let us consider the power series
$$\frac{1}{1-2x-x^2} = \sum_{n=0}^{\infty} a_n x^n.$$
Prove that for every positive integer n, there exists a positive integer m so that
$$a_n^2 + a_{n+1}^2 = a_m.$$

9. Let $(f_n)_{n\geq 1}$ be the Fibonacci sequence given by the recurrence
$$f_{n+2} = f_{n+1} + f_n, \quad n \in \mathbb{N},$$
where $f_1 = f_2 = 1$. Prove that for every integer $n \geq 1$, we have
$$f_{3n} = f_{n+1}^3 + f_n^3 - f_{n-1}^3.$$

10. Let $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in M_2(\mathbb{R})$. Prove that there exist two sequences $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$ such that

$$A^n = \begin{pmatrix} a_n & b_n \\ b_n & a_n \end{pmatrix},$$

for all positive integers n. Find the general terms of these sequences.

11. Let $X = \begin{pmatrix} t & u \\ v & w \end{pmatrix}$ be a second order complex matrix. For every natural number n, let us denote $X^n = \begin{pmatrix} t_n & u_n \\ v_n & w_n \end{pmatrix}$; $a = t+w$ and $b = tw-uv$ are the trace, respectively the determinant of X. Prove that the following are equivalent:

(i) Each of the sequences $(t_n)_{n\geq 1}$, $(u_n)_{n\geq 1}$, $(v_n)_{n\geq 1}$, and $(w_n)_{n\geq 1}$ is convergent.

(ii) One of the following holds:

- $X = I_2$ (the identity matrix), or
- $a = b + 1$ and b has absolute value less than 1, or
- $|a|^2 + |a^2 - 4b| < 2(|b|^2 + 1) < 4$.

Solutions

1. a) We have for all integers $n \geq 1$,

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}^{n-1}$$

and

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+1} & a_{n+2} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_3 \end{pmatrix} \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}^{n-1}.$$

By considering the determinant, we obtain

$$a_n a_{n+3} - a_{n+1} a_{n+2} = (a_1 a_4 - a_2 a_3) q^{n-1},$$

respectively

$$a_n a_{n+2} - a_{n+1}^2 = (a_1 a_3 - a_2^2) q^{n-1}.$$

By dividing, we deduce that

$$\frac{a_n a_{n+3} - a_{n+1} a_{n+2}}{a_n a_{n+2} - a_{n+1}^2} = \frac{a_1 a_4 - a_2 a_3}{a_1 a_3 - a_2^2}.$$

b) Let us denote

$$p = \frac{a_n a_{n+3} - a_{n+1} a_{n+2}}{a_n a_{n+2} - a_{n+1}^2}.$$

It follows that

$$a_n a_{n+3} - a_{n+1} a_{n+2} = p(a_n a_{n+2} - a_{n+1}^2),$$

thus

$$a_n(a_{n+3} - pa_{n+2}) = a_{n+1}(a_{n+2} - pa_{n+1}),$$

or

$$\frac{a_{n+2} - pa_{n+1}}{a_n} = \frac{a_{n+3} - pa_{n+2}}{a_{n+1}}.$$

This relation says that the sequence $\left(\frac{a_{n+2} - pa_{n+1}}{a_n}\right)_{n\geq 1}$ is constant, and if we denote by q the common value of a term of the sequence, we derive

$$\frac{a_{n+2} - pa_{n+1}}{a_n} = q.$$

Hence

$$a_{n+2} = pa_{n+1} + qa_n.$$

2. a) By considering the matrix X_n associated with the given recurrence relation, we obtain

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & p \end{pmatrix}^{n-1},$$

for all positive integers n. By considering the determinant, it follows

$$a_n a_{n+3} - a_{n+1} a_{n+2} = (a_1 a_4 - a_2 a_3)(-1)^{n-1},$$

so $\lambda = -(a_1 a_4 - a_2 a_3)$.

b) By considering the matrix Y_n associated with the given recurrence relation, we obtain

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+1} & a_{n+2} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & p \end{pmatrix}^{n-1},$$

for all integers $n \geq 1$. By considering the determinant, it follows

$$a_n a_{n+2} - a_{n+1}^2 = (a_1 a_3 - a_2^2)(-1)^{n-1},$$

so $\mu = -(a_1 a_3 - a_2^2)$.

3. For all positive integers n, we have

$$\begin{vmatrix} a_{n-1}+a_{n+1} & a_n+a_{n+2} \\ a_n & a_{n+1} \end{vmatrix} = \begin{vmatrix} a_{n-1} & a_n \\ a_n & a_{n+1} \end{vmatrix} + \begin{vmatrix} a_{n+1} & a_{n+2} \\ a_n & a_{n+1} \end{vmatrix}$$
$$= -1+1=0.$$

Hence

$$a_{n+1}(a_{n-1}+a_{n+1}) = a_n(a_n+a_{n+2}).$$

or

$$\frac{a_{n-1}+a_{n+1}}{a_n} = \frac{a_n+a_{n+2}}{a_{n+1}},$$

for all positive integers n. Thus the sequence $\left(\frac{a_{n-1}+a_{n+1}}{a_n}\right)_{n\in\mathbb{N}}$ is a constant sequence. If we denote by λ the common value of its terms, then

$$\frac{a_{n-1}+a_{n+1}}{a_n} = \lambda \Leftrightarrow a_{n+1} = \lambda a_n - a_{n-1}.$$

4. We have, for all integers $n \geq 2$,

$$A\cdot B^{n-1} = \begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} = \begin{pmatrix} a_{n-1} & a_n \\ a_{n+1} & a_{n+2} \end{pmatrix}\cdot B.$$

If we denote

$$B = \begin{pmatrix} p & q \\ r & s \end{pmatrix},$$

then

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} = \begin{pmatrix} a_{n-1} & a_n \\ a_{n+1} & a_{n+2} \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix}$$

or

$$\begin{pmatrix} a_n & a_{n+1} \\ a_{n+2} & a_{n+3} \end{pmatrix} = \begin{pmatrix} pa_{n-1}+qa_n & ra_{n-1}+sa_n \\ pa_{n+1}+qa_{n+2} & ra_{n+1}+sa_{n+2} \end{pmatrix}.$$

By identifying the entries, we obtain

$$a_{n+1} = sa_n + ra_{n-1},$$

which is a second order recurrence.

5. The problem is solved if we recognize and prove the relation

$$a_{2n+3} = a_n a_{n+1} + a_{n+1}a_{n+2}.$$

The given sequence is given by a recurrence relation of the second order with $p=-2$, $q=-1$, so let us denote

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

For every positive integer n we have

$$A^{n+2} = \begin{pmatrix} a_n & a_{n+1} \\ a_{n+1} & a_{n+2} \end{pmatrix},$$

which can be also verified by induction. Further, the matrix equality

$$A^{n+2} \cdot A^{n+2} = A^{2n+4},$$

reads

$$\begin{pmatrix} a_n^2 + a_{n+1}^2 & a_n a_{n+1} + a_{n+1} a_{n+2} \\ a_n a_{n+1} + a_{n+1} a_{n+2} & a_{n+1}^2 + a_{n+2}^2 \end{pmatrix} = \begin{pmatrix} a_{2n+2} & a_{2n+3} \\ a_{2n+3} & a_{2n+4} \end{pmatrix},$$

and the desired conclusion follows by identification of the entries from the first row and the second column.

6. The given sequence satisfies a second order recurrence relation with $p = -1$, $q = -1$, so it is natural to consider the matrix

$$\Omega = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Similarly, we obtain

$$\begin{pmatrix} L_n & L_{n+1} \\ L_{n+1} & L_{n+2} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n.$$

By multiplying to the left with

$$\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}^{-1} = \frac{1}{5} \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix},$$

we deduce

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \frac{1}{5} \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} L_n & L_{n+1} \\ L_{n+1} & L_{n+2} \end{pmatrix}.$$

By replacing in the equality

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{2n} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n,$$

it results in

$$\frac{1}{5} \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} L_{2n} & L_{2n+1} \\ L_{2n+1} & L_{2n+2} \end{pmatrix}$$

$$= \frac{1}{5} \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} L_n & L_{n+1} \\ L_{n+1} & L_{n+2} \end{pmatrix} \cdot \frac{1}{5} \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} L_n & L_{n+1} \\ L_{n+1} & L_{n+2} \end{pmatrix},$$

and by simplifying at left,

$$5\begin{pmatrix} L_{2n} & L_{2n+1} \\ L_{2n+1} & L_{2n+2} \end{pmatrix} = \begin{pmatrix} L_n & L_{n+1} \\ L_{n+1} & L_{n+2} \end{pmatrix}\begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} L_n & L_{n+1} \\ L_{n+1} & L_{n+2} \end{pmatrix}.$$

After some computations, we obtain

$$5\begin{pmatrix} L_{2n} & L_{2n+1} \\ L_{2n+1} & L_{2n+2} \end{pmatrix}$$

$$= \begin{pmatrix} 3L_n - L_{n+1} & -L_n + 2L_{n+1} \\ 3L_{n+1} - L_{n+2} & -L_{n+1} + 2L_{n+2} \end{pmatrix}\begin{pmatrix} L_n & L_{n+1} \\ L_{n+1} & L_{n+2} \end{pmatrix}.$$

By identifying the entries from the first row and the first column and using the recurrence relation, we obtain

$$\begin{aligned} 5L_{2n} &= (3L_n - L_{n+1})\,L_n + (-L_n + 2L_{n+1})\,L_{n+1} \\ &= 3L_n^2 - 2L_nL_{n+1} + 2L_{n+1}^2 \\ &= 2L_n^2 + (L_n^2 - 2L_nL_{n+1} + L_{n+1}^2) + L_{n+1}^2 \\ &= 2L_n^2 + (L_{n+1} - L_n)^2 + L_{n+1}^2 \\ &= 2L_n^2 + L_{n-1}^2 + L_{n+1}^2. \end{aligned}$$

By identifying the entries from the first row and the second column and using the recurrence relation, we obtain

$$\begin{aligned} 5L_{2n+1} &= (3L_n - L_{n+1})\,L_{n+1} + (-L_n + 2L_{n+1})\,L_{n+2} \\ &= 3L_nL_{n+1} - L_{n+1}^2 - L_nL_{n+2} + 2L_{n+1}L_{n+2} \\ &= 3L_nL_{n+1} - L_{n+1}^2 - L_n(L_n + L_{n+1}) + 2L_{n+1}(L_n + L_{n+1}) \\ &= L_{n+1}^2 + 4L_nL_{n+1} - L_n^2 \\ &= (L_{n+1}^2 + 2L_nL_{n+1} + L_n^2) + 2L_nL_{n+1} - 2L_n^2 \\ &= (L_n + L_{n+1})^2 + 2L_n(L_{n+1} - L_n) \\ &= L_{n+2}^2 + 2L_nL_{n-1}. \end{aligned}$$

7. For all integers $n \geq 0$,

$$\begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n,$$

thus

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix}.$$

By replacing in the identity

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{2n} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n},$$

we obtain

$$\begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} F_{2n} & F_{2n+1} \\ L_{2n} & L_{2n+1} \end{pmatrix}$$

$$= \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix}.$$

Hence

$$\begin{aligned} \begin{pmatrix} F_{2n} & F_{2n+1} \\ L_{2n} & L_{2n+1} \end{pmatrix} &= \begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix} \\ &= \begin{pmatrix} -F_n + 2F_{n+1} & F_n - F_{n+1} \\ -L_n + 2L_{n+1} & L_n - L_{n+1} \end{pmatrix} \begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix} \\ &= \begin{pmatrix} F_{n-1} + F_{n+1} & -F_{n-1} \\ L_{n-1} + L_{n+1} & -L_{n-1} \end{pmatrix} \begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix}, \end{aligned}$$

thus

$$\begin{pmatrix} F_{2n} & F_{2n+1} \\ L_{2n} & L_{2n+1} \end{pmatrix} = \begin{pmatrix} F_{n-1} + F_{n+1} & -F_{n-1} \\ L_n + L_{n+1} & -L_{n-1} \end{pmatrix} \begin{pmatrix} F_n & F_{n+1} \\ L_n & L_{n+1} \end{pmatrix}.$$

8. By using

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n,$$

we have

$$\begin{aligned} \frac{1}{1-2x-x^2} &= \frac{1}{2\sqrt{2}} \left(\frac{1+\sqrt{2}}{1-(1+\sqrt{2})x} - \frac{1-\sqrt{2}}{1-(1-\sqrt{2})x} \right) \\ &= \frac{1+\sqrt{2}}{2\sqrt{2}} \cdot \frac{1}{1-(1+\sqrt{2})x} - \frac{1-\sqrt{2}}{2\sqrt{2}} \cdot \frac{1}{1-(1-\sqrt{2})x} \\ &= \frac{1+\sqrt{2}}{2\sqrt{2}} \sum_{n=0}^{\infty} \left[(1+\sqrt{2})x\right]^n - \frac{1-\sqrt{2}}{2\sqrt{2}} \sum_{n=0}^{\infty} \left[(1-\sqrt{2})x\right]^n \\ &= \frac{1}{2\sqrt{2}} \sum_{n=0}^{\infty} (1+\sqrt{2})^{n+1} x^n - \frac{1}{2\sqrt{2}} \sum_{n=0}^{\infty} (1-\sqrt{2})^{n+1} x^n. \end{aligned}$$

It follows that

$$a_n = \frac{1}{2\sqrt{2}} \left((1+\sqrt{2})^{n+1} - (1-\sqrt{2})^{n+1} \right)$$

and consequently,

$$a_{n+1} - 2a_n - a_{n-1} = 0.$$

As we have already seen, it is natural to consider the matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

By induction,

$$A^{n+2} = \begin{pmatrix} a_n & a_{n+1} \\ a_{n+1} & a_{n+2} \end{pmatrix}, \ \forall\, n \in \mathbb{N}.$$

Now the conclusion follows from the matrix equality

$$A^{n+2} \cdot A^{n+2} = A^{2n+4}.$$

Indeed, we have

$$\begin{pmatrix} a_n^2 + a_{n+1}^2 & a_n a_{n+1} + a_{n+1}a_{n+2} \\ a_n a_{n+1} + a_{n+1}a_{n+2} & a_{n+1}^2 + a_{n+2}^2 \end{pmatrix} = \begin{pmatrix} a_{2n+2} & a_{2n+3} \\ a_{2n+3} & a_{2n+4} \end{pmatrix},$$

so

$$a_n^2 + a_{n+1}^2 = a_{2n+2}.$$

9. Let us define the matrix

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

By induction,

$$A^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}.$$

Indeed,

$$\begin{aligned} A^{n+1} = A \cdot A^n &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \\ &= \begin{pmatrix} f_{n+1} + f_n & f_n + f_{n-1} \\ f_{n+1} & f_n \end{pmatrix} \\ &= \begin{pmatrix} f_{n+2} & f_{n+1} \\ f_{n+1} & f_n \end{pmatrix}. \end{aligned}$$

Now we write the matrix A^{3n} in two ways,

$$A^{3n} = \begin{pmatrix} f_{3n+1} & f_{3n} \\ f_{3n} & f_{3n-1} \end{pmatrix} \tag{7}$$

and

$$A^{3n} = (A^n)^3 = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}^3$$

$$\begin{pmatrix} f_{n+1}^3 + 2f_{n+1}f_n^2 + f_n^2 f_{n-1} & f_{n+1}^2 f_n + f_{n+1}f_n f_{n-1} + f_n^3 + f_n f_{n-1}^2 \\ f_{n+1}^2 f_n + f_{n+1}f_n f_{n-1} + f_n^3 + f_n f_{n-1}^2 & f_{n+1}f_n^2 + 2f_n^2 f_{n-1} + f_{n-1}^3 \end{pmatrix} \tag{8}$$

Now, by identification of the elements from the secondary diagonal of the matrices in (7) and (8), we derive

$$f_{3n} = f_{n+1}^2 f_n + f_{n+1}f_n f_{n-1} + f_n^3 + f_n f_{n-1}^2.$$

Further, using the recurrence relation, we have

$$\begin{aligned} f_{3n} &= f_{n+1}f_n(f_{n+1} + f_{n-1}) + f_n^3 + f_n f_{n-1}^2 \\ &= f_{n+1}(f_{n+1} - f_{n-1})(f_{n+1} + f_{n-1}) + f_n^3 + f_n f_{n-1}^2 \\ &= f_{n+1}(f_{n+1}^2 - f_{n-1}^2) + f_n^3 + f_n f_{n-1}^2 \\ &= f_{n+1}^3 - f_{n+1}f_{n-1}^2 + f_n^3 + f_n f_{n-1}^2 \\ &= f_{n+1}^3 + f_n^3 - f_{n-1}^2(f_{n+1} - f_n) \\ &= f_{n+1}^3 + f_n^3 - f_{n-1}^3. \end{aligned}$$

10. Let us consider the relation

$$A^{n+1} = A^n \cdot A$$

or

$$\begin{pmatrix} a_{n+1} & b_{n+1} \\ b_{n+1} & a_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ b_n & a_n \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} a_n + 2b_n & 2a_n + b_n \\ 2a_n + b_n & a_n + 2b_n \end{pmatrix}.$$

Hence

$$\begin{cases} a_{n+1} = a_n + 2b_n \\ b_{n+1} = 2a_n + b_n \end{cases}.$$

These recurrence relations together with the initial values

$$a_1 = 1, \quad b_1 = 2$$

uniquely define the sequences $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$. By induction, these sequences confirm the assertion in the problem. By adding, then subtracting the recurrence relations, we obtain

$$\begin{aligned} a_{n+1} + b_{n+1} &= 3(a_n + b_n) \\ a_{n+1} - b_{n+1} &= (-1)(a_n - b_n) \end{aligned}$$

Hence the sequences $(a_n + b_n)_{n\geq 1}$ and $(a_n - b_n)_{n\geq 1}$ are geometric progressions. We have

$$a_n + b_n = 3^n, \quad a_n - b_n = (-1)^n$$

and consequently,

$$a_n = \frac{3^n + (-1)^n}{2}, \quad b_n = \frac{3^n - (-1)^n}{2}.$$

11. We need two helping results.

Lemma 1. Let z be a complex number. The sequence $(z^n)_{n\geq 1}$ is convergent if and only if either $|z| < 1$ or $z = 1$.

Proof. The "if" part is trivial, thus we pass directly to proving that if the sequence $(z^n)_{n\geq 1}$ is convergent, then either $|z| < 1$, or $z = 1$.

First, from the convergence of the considered sequence the convergence of the sequence $(|z|^n)_{n\geq 1}$ of the absolute values of its terms follows, and this yields $|z| \leq 1$. Thus it remains to show that, if $(z^n)_{n\geq 1}$ converges and $|z| = 1$, then $z = 1$. Let us consider $z = \cos\varphi + i\sin\varphi$, for some $\varphi \in [0, 2\pi)$, hence $z^n = \cos n\varphi + i\sin n\varphi, \forall n \geq 1$. The convergence of a sequence of complex numbers implies the convergence of the sequences of real, respectively imaginary parts of its terms: thus $(x_n)_{n\geq 1}$ and $(y_n)_{n\geq 1}$ defined by

$$x_n = \cos n\varphi \text{ and } y_n = \sin n\varphi, \ \forall n \geq 1$$

must be convergent.

Let us denote by x and y the limits of $(x_n)_{n\geq 1}$ and $(y_n)_{n\geq 1}$, respectively. Of course, x and y are real numbers and we have

$$x_{n+1} = x_n \cos\varphi - y_n \sin\varphi, \ \forall n \geq 1$$

and

$$y_{n+1} = y_n \cos\varphi + x_n \sin\varphi, \ \forall n \geq 1.$$

Passing to the limit for $n \to \infty$ we get

$$\begin{cases} x(1 - \cos\varphi) + y\sin\varphi = 0 \\ -x\sin\varphi + y(1 - \cos\varphi) = 0. \end{cases}$$

On the other hand,

$$x_n^2 + y_n^2 = \cos^2 n\varphi + \sin^2 n\varphi = 1, \ \forall n \geq 1,$$

leads (again by passing to the limit) to $x^2 + y^2 = 1$, therefore x and y cannot be simultaneously zero; that is, the above homogeneous linear system (with unknowns x and y) has nonzero solutions, and consequently its determinant has to be null. This means that

$$(1-\cos\varphi)^2+\sin^2\varphi=0 \Rightarrow \cos\varphi=1 \text{ and } \sin\varphi=0,$$

and thus $z=1$ follows.

Lemma 2. Let a and b be complex numbers, and let z_1 and z_2 be the roots of the equation $z^2-az+b=0$. The following are equivalent:

(α) $|z_1|<1$ and $|z_2|<1$.

(β) $|a|^2+|a^2-4b|<2(|b|^2+1)<4$.

Proof. For the nonnegative real numbers $|z_1|$ and $|z_2|$ to be less than 1 it is both necessary and sufficient to have $(|z_1|^2-1)(|z_2|^2-1)>0$ (that is, to have $|z_1|$ and $|z_2|$ on the same side of 1) and $|z_1z_2|=|z_1||z_2|<1$. We have $z_1z_2=b$, hence the second condition actually says that $|b|<1$, which is equivalent to $2(|b|^2+1)<4$.

We also have $z_1+z_2=a$ and $(z_1-z_2)^2=(z_1+z_2)^2-4z_1z_2=a^2-4b$, thus the first condition, which can also be written as

$$2(|z_1|^2+|z_2|^2)<2(|z_1|^2|z_2|^2+1)$$

is the same as $|a|^2+|a^2-4b|<2(|b|^2+1)$, because of the well-known identities $2(|z_1|^2+|z_2|^2)=|z_1+z_2|^2+|z_1-z_2|^2$ and $|z_1z_2|=|z_1||z_2|$.

Back to the problem now. Note that by the Cayley–Hamilton theorem,

$$X^2-aX+bI_2=O_2$$

(where O_2 is the zero matrix of order 2), therefore

$$X^{n+2}-aX^{n+1}+bX^n=O_2,\ \forall n\geq 1,$$

which shows that any of the sequences $(t_n)_{n\geq 1}$, $(u_n)_{n\geq 1}$, $(v_n)_{n\geq 1}$ and $(w_n)_{n\geq 1}$ verifies one and the same second order linear recurrence relation

$$x_{n+2}-ax_{n+1}+bx_n=0,\ \forall n\geq 1.$$

So, if we denote by T, U, V, W the limits of these sequences (if they exist and are finite), by passing to the limit, we obtain

$$T-aT+bT=U-aU+bU=V-aV+bV=W-aW+bW=0.$$

Now we prove the implication (i)⇒(ii). Thus we assume that for a given matrix X, the corresponding sequences $(t_n)_{n\geq 1}$, $(u_n)_{n\geq 1}$, $(v_n)_{n\geq 1}$, and

$(w_n)_{n\geq 1}$ are convergent (and have limits T, U, V, and W, respectively). The convergence of sequences $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$ defined by

$$a_n = t_n + w_n = \mathrm{tr}(X^n)$$

and

$$b_n = t_n w_n - u_n v_n = \det(X^n)$$

for all $n \in \mathbb{N}^*$ follows (with limits $A = T + W$ and $B = TW - UV$, respectively). We have

$$\det(X^n) = (\det(X))^n \Rightarrow b_n = b^n, \ \forall n \geq 1,$$

and lemma 1 implies that b is either equal to 1, or a number with its absolute value less than 1.

Consider first the case $b = 1$. The recurrence relation verified by each of the four sequences now becomes

$$x_{n+2} - a x_{n+1} + x_n = 0, \ \forall n \geq 1,$$

while for their limits, we have

$$T - aT + T = U - aU + U = V - aV + V = W - aW + W = 0$$

$$\Rightarrow (2-a)T = (2-a)U = (2-a)V = (2-a)W = 0.$$

We also get

$$t_n w_n - u_n v_n = b^n = 1, \ \forall n \geq 1,$$

whence $TW - UV = 1$ follows, therefore T, U, V, W cannot be all null. Then, necessarily, $a = 2$ and a simple induction shows that

$$X^n = I_2 + n(X - I_2), \ \forall n \geq 1.$$

This immediately implies

$$t_n = 1 + n(t-1), u_n = nu, v_n = nv, w_n = 1 + n(w-1),$$

for every $n \in \mathbb{N}^*$; it is now clear that the hypothesis on the convergence of all sequences $(t_n)_{n\geq 1}$, $(u_n)_{n\geq 1}$, $(v_n)_{n\geq 1}$, and $(w_n)_{n\geq 1}$ leads to $t = 1$, $u = 0$, $v = 0$ and $w = 1$, that is, to $X = I_2$. Assume further that b is a complex number with absolute value less than 1.

Let us consider yet the roots z_1 and z_2 of the equation $z^2 - az + b = 0$ (the eigenvalues of matrix X). It is well-known that

$$a_n = \mathrm{tr}(X^n) = z_1^n + z_2^n, \ \forall n \geq 1$$

and, also, that $z_1 z_2 = b$, hence

$$|z_1||z_2| = |b| < 1.$$

This means that at least one of z_1 and z_2 has absolute value less than 1. If, for example, $|z_1| < 1$, then $(z_1^n)_{n\geq 1}$ is convergent (with limit 0); on the other hand, the sequence of traces of matrices X^n must be convergent, meaning that the sequence $(z_1^n + z_2^n)_{n\geq 1}$ is convergent, too. Consequently, the sequence with general term

$$z_2^n = (z_1^n + z_2^n) - z_1^n,$$

is convergent, hence (by lemma 1, again) either $z_2 = 1$ or $|z_2| < 1$. In summary, if $|b| < 1$, then either both roots of the characteristic equation of matrix X have absolute values less than 1, or one of them has absolute value less than 1, while the other equals 1. In this second case (assume $|z_1| < 1$ and $z_2 = 1$), we obviously get $b = z_1$ and $a = z_1 + z_2 = b + 1$ (with $|b| < 1$), that is, the second situation from (ii).

Otherwise, if $|z_1| < 1$ and $|z_2| < 1$, by lemma 2, we infer that

$$|a|^2 + |a^2 - 4b| < 2(|b|^2 + 1) < 4$$

and thus we fall into the third case of (ii).

It only remains to prove (ii)$\Rightarrow$(i). For $X = I_2$ we have

$$X^n = I_2 \Rightarrow t_n = w_n = 1, u_n = v_n = 0, \ \forall n \geq 1$$

and the convergence of the four sequences is clear.

If matrix X has $a = \operatorname{tr}(X) = \det(X) + 1 = b + 1$ and $|b| < 1$, then one of its eigenvalues is 1 and the other is b (with absolute value less than 1). In this case, one easily checks that

$$X^n = \frac{1}{b-1}[b^n(X - I_2) + bI_2 - X], \forall n \geq 1,$$

which leads to formulas like

$$x_n = cb^n + d, \ \forall n \geq 1$$

for $(x_n)_{n\geq 1}$ being any of the four sequences $(t_n)_{n\geq 1}$, $(u_n)_{n\geq 1}$, $(v_n)_{n\geq 1}$, and $(w_n)_{n\geq 1}$ (with constant cs and ds depending on X, and, of course, not necessarily the same for all sequences). As $\lim\limits_{n\to\infty} b^n = 0$, the convergence of any of the four sequences follows.

Finally, the third situation implies, based on lemma 2, that the solutions z_1 and z_2 of the characteristic equation of matrix X are complex numbers with absolute values less than 1. This is also the characteristic equation of the recurrence verified by each of the sequences $(t_n)_{n\geq 1}$, $(u_n)_{n\geq 1}$, $(v_n)_{n\geq 1}$, and $(w_n)_{n\geq 1}$. Thus, for the general term of any of these sequences (which we denote, again, by x_n), we have a formula like

$$x_n = cz_1^n + dz_2^n,\ \forall n \geq 1$$

(when $z_1 \neq z_2$), or

$$x_n = (c + nd)z_1^n,\ \forall n \geq 1$$

(for $z_1 = z_2$). As $|z_1| < 1$ and $|z_2| < 1$, we get

$$\lim_{n\to\infty} z_1^n = \lim_{n\to\infty} z_2^n = 0 \text{ and } \lim_{n\to\infty} nz_1^n = 0,$$

whence the convergence of the four sequences again follows easily (each of them with limit zero), finishing the proof.

Chapter 14

Final Problem Set

We close our book with a few more problems — related, of course, to the topics that we have discussed. Some of them are simple, and some are pretty hard; their choice depended much on our taste and preferences. Anyway, we hope that the interested reader will enjoy this final challenge, trying to solve the problems independently, based (more or less; hopefully more) on what he or she learned by reading the book. Nevertheless, it is always worthwhile to remember that studying mathematics is a never-ending story, therefore we wish you luck not only with these, but with any problem that you will have to solve on the long and winding road of this continuous and fascinating study.

Proposed Problems

1. We color each point of the plane with one of n given colors. Prove that there exists a rectangle with vertices of the same color.

2. Let a and b be positive integers. Show that there are positive integers s and t such that $an+s$ and $bn+t$ are relatively prime for any integer n.

3. Let a and b be relatively prime integers, and let $(x_n)_{n\geq 1}$ be the sequence of integers defined by $x_0=0$, $x_1=1$, and $x_n=ax_{n-1}+bx_{n-2}$ for every $n\geq 2$. Prove that $(x_m, x_n)=x_{(m,n)}$ for all natural numbers m and n.

4. a) Prove that there are no four consecutive natural numbers such that all four can be expressed as sums of two squares.

   b) Prove that there are infinitely many triples of consecutive natural numbers such that each member of such a triple is the sum of two squares.

5. A positive integer is called *square-free* if it is not divisible by the square of any integer greater than 1 (or, equivalently, if it is either 1 or a product

of distinct prime factors — possibly one single prime factor). If $(l_n)_{n\geq 1}$ is the sequence of the square-free positive integers in increasing order ($l_1 = 1$, $l_2 = 2$, $l_3 = 3$, $l_4 = 5$, $l_5 = 6$, and so on) it is well-known (and you do *not* have to prove) that

$$\lim_{n\to\infty} \frac{l_n}{n} = \frac{\pi^2}{6}.$$

Show that there are infinitely many triples of consecutive natural numbers such that every member of any of these triples is square-free.

6. Let a, b, c, and d be positive integers such that $(a, c) = 1$ and ac is not a square. Prove that there are infinitely many integers n such that $an + b^2$ and $cn + d^2$ are both squares.

7. Let n be a positive integer not divisible by 3, and let $s \geq n - 1$ be an integer. Prove that there exists a positive integer N divisible by n and having the sum of digits $S(N) = s$.

8. Let an arithmetic progression of positive integers be given. Prove that one can find a subsequence of this arithmetic progression that is a geometric progression.

9. Let α be a positive irrational number and let n_0 be a positive integer. Prove that the sequence $([n\alpha])_{n\geq n_0}$ contains arbitrarily long arithmetic progressions.

10. Let α, β, and γ be three positive real numbers, and let

$$A = \{[n\alpha] \mid n \in \mathbb{N}^*\},\ B = \{[n\beta] \mid n \in \mathbb{N}^*\},\ C = \{[n\gamma] \mid n \in \mathbb{N}^*\}.$$

Prove that the sets A, B, and C cannot partition the set $\mathbb{N}^*$ of positive integers.
(That is, we cannot have $A \cup B \cup C = \mathbb{N}^*$ and $A \cap B = A \cap C = B \cap C = \emptyset$ simultaneously.)

11. Let $f(x) = x^2 + ax + b$ be a quadratic function with integer coefficients having the property that the values of f for any two consecutive integers are consecutive squares. Prove that $f(n)$ is a square for any integer n.

12. Let f, g, and h be three quadratic functions such that each of $f - g$, $g - h$, $h - f$ is still a quadratic function (thus with nonzero coefficient of x^2) having equal zeros. Prove that the functions $f - g$, $g - h$, and $h - f$ have a common zero.

13. Let $f(x) = x^2 + ax + b$ and $g(x) = x^2 + cx + d$ be two quadratic functions with real coefficients. We say that the corresponding equations $f(x) = 0$ and $g(x) = 0$ are *friends* if they have real and separated roots (see also problem 2 in the chapter *Quadratic Functions and Quadratic Equations*). Prove that the equations $f(x) = 0$ and $g(x) = 0$ are friends if and only if
$$R = (b - d)^2 + (a - c)(ad - bc) < 0.$$

14. a) (Hedgehog's lemma) Let P be a convex polyhedron in the three-dimensional space. A vector perpendicular to each face of P is considered, having the length equal to the area of that face, and such that all vectors are oriented towards the exterior of the polyhedron. Prove that the sum of all vectors is $\overrightarrow{0}$.

    b) Let a, b, c, and d be positive real numbers such that each of them is less than the sum of the other three. Prove that a tetrahedron exists such that the areas of its faces are precisely a, b, c, and d.

15. Let $A_1A_2A_3A_4$ be a tetrahedron, and let K_j denote the area of its face opposite vertex A_j, for $1 \leq j \leq 4$ (thus K_1 is the area of $A_2A_3A_4$, etc.). Prove that if $K_1 = K_2$ and $K_3 = K_4$, then $A_1A_3 = A_2A_4$ and $A_1A_4 = A_2A_3$.

16. Let $A_1B_1C_1$ and $A_2B_2C_2$ be two distinct equilateral triangles sharing the same center and having the same orientation. Prove that the lines A_1A_2, B_1C_2, and B_2C_1 are concurrent.

17. Let p, q, and r be positive real numbers with $p + q + r = 1$, and let $(x_n)_{n\geq 0}$, $(y_n)_{n\geq 0}$, and $(z_n)_{n\geq 0}$ be the sequences of real numbers defined by $x_0 = 1$, $y_0 = 0$, $z_0 = 0$, and the recurrence relations
$$\begin{aligned} x_n &= px_{n-1} + ry_{n-1} + qz_{n-1} \\ y_n &= qx_{n-1} + py_{n-1} + rz_{n-1} \\ z_n &= rx_{n-1} + qy_{n-1} + pz_{n-1}, \end{aligned}$$
for all $n \geq 1$. Prove that $(x_n)_{n\geq 0}$, $(y_n)_{n\geq 0}$, and $(z_n)_{n\geq 0}$ are convergent and determine their limits.

Solutions

1. We look at the points with integer coordinates (which are called *lattice points*, that is, the points at which the lines of equations $x = a$ and $y = b$, with integers a and b intersect; we say the lines form a *lattice*). We choose a vertical line L_1, say of equation $x = x_1$ for a fixed (but under no special

condition) integer x_1. Because there are infinitely many lattice points on L_1, each colored with one of the given n colors, there must be infinitely many of these points having the same color. We only need $n^n + 1$ of them, say those having coordinates $(x_1, y_k^{(1)})$, $1 \le k \le n^n + 1$.

Choose further some integer $x_2 \neq x_1$, and look at the points of coordinates $(x_2, y_k^{(1)})$, $1 \le k \le n^n + 1$ situated at the intersections of the (also vertical) line L_2 of equation $x = x_2$ with the horizontal lines of equations $y = y_k^{(1)}$. Their number is $n^n + 1$ and they are colored with n colors, so (by the general pigeonhole principle) we can choose (at least) $n^{n-1} + 1$ of them that have the same color. Let $(x_2, y_k^{(2)})$, $1 \le k \le n^{n-1} + 1$ be the coordinates of these points (note that $y_k^{(2)}$ are $n^{n-1} + 1$ distinct numbers among the initial $y_k^{(1)}$, $1 \le k \le n^n + 1$).

Then look at a new vertical line L_3, of equation $x = x_3$ (with x_3 different from either of x_1 and x_2), and look at the corresponding points on it having coordinates $(x_3, y_k^{(2)})$, $1 \le k \le n^{n-1}+1$. There are $n^{n-1}+1$ points of n possible colors, hence we can find $n^{n-2} + 1$ of them colored with the same color — say their coordinates are $(x_3, y_k^{(3)})$, $1 \le k \le n^{n-2} + 1$. Observe that the intersections of the horizontal lines of equations $y = y_k^{(3)}$, $1 \le k \le n^{n-2}+1$ with each of the vertical lines L_1, L_2, and L_3 have the same color — but not necessarily the same color on L_1 and L_2, or on L_1 and L_3, or on L_2 and L_3 (if this was the case, we would already have found the rectangle with the vertices of the same color).

Clearly, we go on like this by building $n+1$ vertical lines L_j of equations $x = x_j$, $1 \le j \le n+1$ (with mutually distinct $x_1, \ldots, x_{n+1}$), and finding (always by the general pigeonhole principle) on each line L_j points of coordinates $(x_j, y_k^{(j)})$, $1 \le k \le n^{n-j+1} + 1$ that share the same color, and such that their ordinates have the property that

$$\{y_1^{(j+1)}, \ldots, y_{n^{n-j}+1}^{(j+1)}\} \subseteq \{y_1^{(j)}, \ldots, y_{n^{n-j+1}+1}^{(j)}\}$$

for every $1 \le j \le n$.

Thus, on L_{n+1} we obtained two points with the same color, with coordinates $(x_{n+1}, y_1^{(n+1)})$ and $(x_{n+1}, y_2^{(n+1)})$. The intersections of the horizontal lines $\Lambda_1 : \ y = y_1^{(n+1)}$ and $\Lambda_2 : \ y = y_2^{(n+1)}$ with every vertical line L_j, $1 \le j \le n+1$ are two points of the same color. But there are $n + 1$ vertical lines and only n colors, so, by the pigeonhole principle one last time, there must be two of these lines such that their intersections with Λ_1 and Λ_2 have (all four of them) the same color. These four points are the vertices of a rectangle, and share the same color, thus finishing the proof.

2. Let $d = (a, b)$ be the greatest common divisor of a and b, and let a_1 and b_1 be the relatively prime positive integers such that $a = da_1$ and $b = db_1$. We know that there exist positive integers s and t such that $ta_1 - sb_1 = 1$. We claim that s and t thus defined are those for which we are looking.

   Indeed, we have $a_1 b = b_1 a (= da_1 b_1)$, thus, for every integer n,

   $$a_1(bn + t) - b_1(an + s) = ta_1 - sb_1 = 1.$$

   From this equality we see that any common divisor of $an + s$ and $bn + t$ must divide 1, and this is what we wanted to prove.

   For example, if $a = 48 = 6 \cdot 8$ and $b = 114 = 6 \cdot 19$, we can choose $s = 3$ and $t = 7$ and we have

   $$19(48n + 3) - 8(114n + 7) = 1$$

   hence $(48n + 3, 114n + 7) = 1$ for every integer n.

3. Note first that $(x_n, b) = 1$ for every $n \geq 1$. Indeed, we have $(x_1, b) = 1$, and if, for some $n \geq 2$, d is a common divisor for x_n and b, the equality $x_n = ax_{n-1} + bx_{n-2}$ shows that d divides ax_{n-1}, thus x_{n-1}, too (because a and b are relatively prime and d divides b, d is also relatively prime to a). Going backwards, inductively, we get that d divides x_1, hence $d = 1$.

   Also, by induction, $(x_n, x_{n-1}) = 1$ follows for every $n \geq 1$. Indeed, from the recurrence relation we see that a common divisor of x_n and x_{n-1} divides bx_{n-2}, too. But, according to what we just proved, that common divisor is relatively prime to b (since it divides x_n and $(x_n, b) = 1$), hence it actually divides x_{n-2} — thus being a common divisor for x_{n-1} and x_{n-2}. So, if $(x_{n-1}, x_{n-2}) = 1$, then we also have $(x_n, x_{n-1}) = 1$ (and $(x_1, x_0) = 1$ is trivial), consequently, $(x_n, x_{n-1}) = 1$ is true for all $n \geq 1$.

   Then, the general theory of linear and homogeneous recurrences of the second order (or, again, a simple induction) gives $x_n = (\alpha^n - \beta^n)/(\alpha - \beta)$, where α and β are the roots of the characteristic equation $x^2 = ax + b$ (assume for the moment that $\alpha \neq \beta$). It follows that

   $$\frac{x_{kn}}{x_n} = \frac{\alpha^{kn} - \beta^{kn}}{\alpha^n - \beta^n} = \alpha^{(k-1)n} + \alpha^{(k-2)n}\beta^n + \cdots + \beta^{(k-1)n}$$

   is an integer, as being, at the same time, a rational number (because x_{kn} and x_n are integers) and an algebraic integer (because α and β are algebraic integers, being solutions of the equation $x^2 - ax - b = 0$, with integers a and b). Actually, the same formula works for $\alpha = \beta$, in the sense that, in that case, we have $x_n = n\alpha^{n-1}$ — which can be obtained from the above formula by passing to the limit for $\beta \to \alpha$ (anyway, if a and b are relatively prime, there are very few cases when this happens — we invite the reader to figure out which these are). Thus, $x_{kn}/x_n = k\alpha^{(k-1)n}$, and the same reasoning applies in this situation, too, in order to get that x_{kn}/x_n is an integer. Therefore, in any case, if n divides m, then x_n divides x_m (of course, for $n \geq 1$).

Finally, the equality

$$x_m = x_k x_{m+1-k} + b x_{k-1} x_{m-k}$$

can be easily proven by induction over k for every $m \geq 1$ and $1 \leq k \leq m$. (This relation is also helpful for proving that x_n divides x_m whenever n divides m.)

Now let m and n be arbitrary natural numbers, $m \geq n$, and let us divide m by n. Thus $m = cn + r$, with natural numbers c and n, $0 \leq r < n$; we have

$$x_m = x_{cn} x_{m+1-cn} + b x_{cn-1} x_{m-cn} \Leftrightarrow x_m = x_{cn} x_{r+1} + b x_{cn-1} x_r.$$

From here we see that every common divisor of x_n (hence of x_{cn}, too) and x_r also divides x_m. Conversely, if d is a common divisor of x_m and x_n, d also divides x_{cn}, therefore it divides $b x_{cn-1} x_r$. But d is relatively prime to b (since it is a divisor of x_n) and it is relatively prime to x_{cn-1} (as a divisor of x_{cn} — and we know that x_{cn-1} and x_{cn} are relatively prime). It remains that d divides x_r, consequently any common divisor of x_m and x_n is also a common divisor of x_n and x_r (and the converse is also true), meaning that $(x_m, x_n) = (x_n, x_r)$. We use now the Euclidean algorithm for m and n together with this property in order to get the desired conclusion $(x_m, x_n) = x_{(m,n)}$.

Or, as we have seen in the chapter *A Property of the Greatest Common Divisor*, we can expedite our proof by replacing the use of the Euclidean algorithm with the fact that natural numbers s and t exist such that $sm - tn = \delta$, δ being the greatest common divisor of m and n. The equality

$$x_{sm} = x_{tn} x_{\delta+1} + x_{tn-1} x_\delta$$

shows that any common divisor of x_m and x_n (which, as we know, also divides x_{sm} and x_{tn}) divides x_δ, too. Conversely, it is clear that x_δ is a common divisor of x_m and x_n, hence $x_\delta = (x_m, x_n)$ follows, which we intended to prove.

This problem generalizes the well-known fact that the Fibonacci sequence $(F_n)_{n\geq 0}$ (defined by $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for each

$n \geq 2$) has the property that $(F_m, F_n) = F_{(m,n)}$ for all natural numbers m and n. Also, specializing for $a = 2$ and $b = 1$ we find a part of problem 11864 proposed by Bakir Farhi in *The American Mathematical Monthly*, 8/2015. A particular case is the fact that $(u^m - 1, u^n - 1) = u^{(m,n)} - 1$ for any positive integers u, m and n ($a = u + 1$, $b = -u$). Or, more generally, if α and β are any distinct complex numbers such that $\alpha + \beta$ and $\alpha\beta$ are relatively prime integers, then the sequence $(x_n)_{n\geq 1}$ defined by $x_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ has the property $(x_m, x_n) = x_{(m,n)}$ for all m and n. For instance, this happens when α and β are distinct relatively prime integers.

4. a) Every square of an integer is congruent to either 0 or 1 modulo 4. Consequently, the sum of two squares can never be 3 modulo 4. However, given any four consecutive natural numbers there is always one of them which is congruent to 3 modulo 4 — hence this one cannot be the sum of two squares.

   b) The smallest such triple is of course $(0, 1, 2)$, and the following is $(8, 9, 10)$.
   If $(n-1, n, n+1)$ is such a triple, we claim that (n^2-1, n^2, n^2+1) is also a triple of consecutive natural numbers with the required property. Indeed, $n^2 = n^2 + 0^2$ and $n^2 + 1 = n^2 + 1^2$ are evidently sums of two squares, while $n^2 - 1$ is also a sum of two squares because $n^2 - 1 = (n-1)(n+1)$, and we know that $n - 1 = a^2 + b^2$, $n + 1 = c^2 + d^2$, thus

   $$n^2 - 1 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2,$$

   (i.e., the product of two sums of squares is always a sum of two squares).

   So, if we start with $(8, 9, 10)$ we get $(80, 81, 82)$, and from this one we obtain $(6560, 6561, 6562)$, and so on. In general, the operation

   $$(n - 1, n, n + 1) \mapsto (n^2 - 1, n^2, n^2 + 1)$$

   always produces a new triple with the desired property from a triple that is already known to have that property. Moreover, if $n > 1$, we clearly get a triple with bigger least member than the initial triple, thus we obtain infinitely many triples of consecutive numbers, each being the sum of two squares.

   Alternatively, we can use the solutions (x_n, y_n) of the Pell equation

   $$x^2 - 2y^2 = 1,$$

   given by $x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n$ ($(x_0, y_0) = (1, 0)$, $(x_1, y_1) = (3, 2)$, $(x_3, y_3) = (17, 12)$, and so on). Then each triple $(x_n^2 - 1, x_n^2, x_n^2 + 1)$ has the required property (and there are infinitely many of them). We only have to explain why the first component is the sum of two squares, and this is easy: we have $x_n^2 - 1 = 2y_n^2 = y_n^2 + y_n^2$.

Finally, probably the simplest argument is to notice that every triple of the form

$$(4n^4 + 4n^2, 4n^4 + 4n^2 + 1, 4n^4 + 4n^2 + 2)$$

has the required property, because

$$4n^4 + 4n^2 = (2n^2)^2 + (2n)^2,\ 4n^4 + 4n^2 + 1 = (2n^2 + 1)^2 + 0^2,$$

and

$$4n^4 + 4n^2 + 2 = (2n^2 + 1)^2 + 1^2.$$

5. Many examples of such triples can be easily found, as $(5, 6, 7)$, or $(13, 14, 15)$ but, unfortunately, there is no chance to solve this problem in a manner similar to the previous one. We will assume, by way of contradiction, that only finitely many triples of square-free consecutive natural numbers exist. This means that we have $l_{n+2} \geq l_n + 3$ for all but finitely many n, say for $n \geq n_0$. This immediately leads to $l_{n+6} \geq l_n + 9$ for all $n \geq n_0$, with equality if and only if there is equality in all inequalities added to get $l_{n+6} \geq l_n + 9$, that is if and only if $l_{n+2} = l_n + 3$, $l_{n+4} = l_{n+2} + 3$, and $l_{n+6} = l_{n+4} + 3$. But these equalities cannot hold simultaneously. Indeed, assume they were all true. Being square-free, l_n cannot be divisible by 4, thus only the following cases remain. If $l_n = 4k + 1$, then $l_{n+2} = l_n + 3 = 4(k + 1)$ would not be square-free. If $l_n = 4k+2$, then $l_{n+4} = l_n + 6 = 4(k+2)$ would not be square-free. And, if $l_n = 4k + 3$, then $l_{n+6} = l_n + 9 = 4(k + 3)$ would not be square-free. So, any way, we get a contradiction; therefore, since at least one of the inequalities $l_{n+2} \geq l_n + 3$, $l_{n+4} \geq l_{n+2} + 3$, and $l_{n+6} \geq l_{n+4} + 3$ is strict, we actually have $l_{n+6} \geq l_n + 10$ for all $n \geq n_0$. Adding side by side $l_{j+6} \geq l_j + 10$ for $j = n_0, n_0 + 6, \ldots, n_0 + 6p - 6$ we get

$$l_{n_0+6p} \geq l_{n_0} + 10p$$

for all $p \geq 0$, or

$$\frac{l_{n_0+6p}}{n_0 + 6p} \geq \frac{l_{n_0}}{n_0 + 6p} + \frac{10p}{n_0 + 6p}.$$

Now take in both sides the limit for $p \to \infty$. Remembering what the statement of the problem gives, namely that $\lim\limits_{n\to\infty} l_n/n = \pi^2/6$, we obtain

$$\frac{\pi^2}{6} \geq \frac{10}{6},$$

obviously a contradiction — showing that, indeed, there are infinitely many triples of consecutive square-free natural numbers. This proof is due to Laurenţiu Panaitopol.

6. First note that if, for an integer p, the equation $ax^2 - cy^2 = p$ has a solution then it has infinitely many. Indeed, let (x_0, y_0) be a solution, so that we have
$$ax_0^2 - cy_0^2 = p,$$
and let (u_n, v_n), $n \in \mathbb{N}$ be the solutions of the Pell equation $x^2 - acy^2 = 1$, that is
$$u_n^2 - acv_n^2 = 1$$
for all $n \geq 0$ (there are infinitely many solutions for the Pell equation because ac is not a perfect square). Multiply side by side the above equalities and rearrange in order to obtain
$$a(x_0u_n + cy_0v_n)^2 - c(ax_0v_n + y_0u_n)^2 = p.$$
Thus $(x_n, y_n) = (x_0u_n + cy_0v_n, ax_0v_n + y_0u_n)$ are infinitely many solutions for $ax^2 - cy^2 = p$.

   Now the equation $ax^2 - cy^2 = ad^2 - cb^2$ obviously has a solution in positive integers, hence it has infinitely many. Let (s_k, t_k), $k \in \mathbb{N}$ be these solutions, hence
$$as_k^2 - ct_k^2 = ad^2 - cb^2 \Leftrightarrow a(s_k^2 - d^2) = c(t_k^2 - b^2)$$
for all $k \geq 0$. Since a and c are relatively prime, it follows that a divides $t_k^2 - b^2$, that is, $t_k^2 - b^2 = an_k$ for some integer n_k. The equation gives then $s_k^2 - d^2 = cn_k$, so we have $an_k + b^2 = t_k^2$ and $cn_k + d^2 = s_k^2$ for all k, finishing the proof.

7. We first suppose that n is not divisible by 3, by 2, and by 5 (i.e., we assume $(n, 30) = 1$). Apart from the case $n = 1$ for which the problem is trivial, because n and 10 are relatively prime, we have $10^{\varphi(n)} \equiv 1 \pmod{n}$, hence $10^{k\varphi(n)} \equiv 1 \pmod{n}$ for every nonnegative integer k.
   Because n and 3 are relatively prime, so are n and 9, thus there exists $b \in \{0, 1, \ldots, n-1\}$ such that $9b \equiv -s \pmod{n}$.
   Also, let $a = s - b \geq s - (n-1) \geq 0$, and take
$$N = \sum_{i=1}^{a} 10^{i\varphi(n)} + \sum_{j=1}^{b} 10^{j\varphi(n)+1},$$

where an empty sum is considered 0 (so if $a = 0$, the first sum is 0, etc.). We clearly have $S(N) = a + b = s$. Also, we have

$$N \equiv a + 10b = s + 9b \equiv 0 \pmod{n};$$

that is, N is a multiple of n with sum of digits s — a number with precisely the required properties.

In the general case, let $n = 2^p 5^q m$, with $(m, 30) = 1$; according to what we just proved, there exists a multiple M of m with $S(M) = s$ (we have $s \geq n - 1 \geq m - 1$). Then $N = 10^{\max\{p,q\}} M$ is a multiple of n with $S(N) = S(M) = s$, and the problem is completely solved.

This problem was short-listed for the 40th International Mathematical Olympiad, in 1999.

8. Let $(a + nd)_{n \geq 0}$, with positive integers a and d be the given progression (we could have $d = 0$, but in that case the problem becomes trivial). Let $\delta = (a, d)$, and let $a = \delta a_1$, and $d = \delta d_1$, with relatively prime positive integers a_1 and d_1. If $d_1 = 1$ the problem is, again, trivial, so we can suppose further that $d_1 \geq 2$. By Euler's theorem, $a_1^{\varphi(d_1)} \equiv 1 \pmod{d_1}$ (where φ denotes Euler's totient function), therefore $a_1^{s\varphi(d_1)+1} \equiv a_1 \pmod{d_1}$ for any nonnegative integer s. In other words,

$$a_1^{s\varphi(d_1)+1} = a_1 + n_s d_1$$

for some nonnegative integer n_s, for all $s \geq 0$.
This means that the subsequence $(a + n_s d)_{s \geq 0}$ of the original arithmetic progression $(a + nd)_{n \geq 0}$ has terms

$$a + n_s d = \delta(a_1 + n_s d_1) = \delta a_1^{s\varphi(d_1)+1}$$

that form a geometric progression (with common ratio $a_1^{\varphi(d_1)}$), which was what we wanted to prove.

9. As usual, $[x]$ and $\{x\}$ denote the integral and the fractional parts of the real number x respectively. We use Kronecker's theorem, according to which the set $\{\{n\alpha\} \mid n \in \mathbb{N}^*\}$ is dense in $[0, 1]$. In particular, given positive integers n_0 and N, there exists a positive integer k (actually infinitely many) such that $k \geq n_0$ and

$$0 < \{k\alpha\} < \frac{1}{N+1}.$$

We then have

$$0 < j\{k\alpha\} < \frac{j}{N+1} < 1$$

for $j = 1, 2, \dots, N$. Since $\{k\alpha\} = k\alpha - [k\alpha]$, we get

$$j[k\alpha] < jk\alpha < j[k\alpha] + 1,$$

meaning that

$$[jk\alpha] = j[k\alpha] \text{ for any such } j.$$

Thus, for $n_j = jk$, $1 \le j \le N$ we have $n_0 \le n_1 < \cdots < n_N$ and $[n_j\alpha] = j[k\alpha]$ are N consecutive terms of an arithmetic progression (having common difference $[k\alpha]$). Since N can be arbitrarily chosen, the problem is solved.

Note that the result remains true for rational α, too, with a much simpler proof (find it!). Actually, in this case, infinite arithmetic progressions can be extracted from the sequence $([n\alpha])_{n\ge n_0}$.

10. Suppose, on the contrary, that for some positive α, β, and γ the sets $A = \{[n\alpha] \mid n \in \mathbb{N}^*\}$, $B = \{[n\beta] \mid n \in \mathbb{N}^*\}$, and $C = \{[n\gamma] \mid n \in \mathbb{N}^*\}$ are mutually disjoint and have their union the set of positive integers. Observe first that, if this is the case, the ratio of any two of α, β, and γ is irrational. For, if we had, say, $\alpha/\beta = m/n$, with positive integers m and n, then $n\alpha = m\beta$, hence $[n\alpha] = [m\beta]$, and finally $A \cap B \ne \emptyset$ would follow — contradiction. In particular, α, β, and γ are distinct, and, by symmetry, we can assume without loss of generality that $0 < \alpha < \beta < \gamma$. Since $x \le y$ implies $[x] \le [y]$, we will have $[n\alpha] \le [n\beta] \le [n\gamma]$ (with actually strict inequalities, because any two of A, B, and C do not have common elements) for any positive integer n. So 1 must belong to A, and this implies $\alpha < 2$ (otherwise $[n\alpha] \ge [\alpha] \ge 2$ for all $n \ge 1$, and 1 would not be in any of A, B, C). Also, we must have $\alpha \ge 1$, because $[\alpha] = [1 \cdot \alpha] \ge 1$. Thus $1 \le \alpha < 2$.

    Now we have

    $$0 \le [(n+1)\alpha] - [n\alpha] = \alpha + \{n\alpha\} - \{(n+1)\alpha\} \le \alpha + \{n\alpha\} < 2 + 1 = 3$$

    and (since $[(n+1)\alpha] - [n\alpha]$ is an integer), actually,

    $$0 \le [(n+1)\alpha] - [n\alpha] \le 2$$

    for all $n \ge 1$. In fact $[(n+1)\alpha] = [n\alpha]$ is not possible, since if it was, there would be some positive integer m with $m \le n\alpha < (n+1)\alpha < m+1$, and this would yield $\alpha < 1$). Thus we finally have

    $$1 \le [(n+1)\alpha] - [n\alpha] \le 2,$$

    therefore between any two consecutive elements of A at most one member of $B \cup C$ can interfere.

We further use the well-known fact that, for any irrational number x, the set $\{mx - n \mid m, n \in \mathbb{N}^*\}$ is dense in $\mathbb{R}$. In particular, as we saw that β/γ is irrational, there exist positive integers p and q such that

$$-\frac{1}{\gamma} < p\frac{\beta}{\gamma} - q < \frac{1}{\gamma} \Leftrightarrow -1 < p\beta - q\gamma < 1.$$

We can rewrite this as

$$\{p\beta\} - \{q\gamma\} - 1 < [p\beta] - [q\gamma] < \{p\beta\} - \{q\gamma\} + 1$$

and, because

$$|\{p\beta\} - \{q\gamma\}| < 1,$$

we infer

$$-2 < [p\beta] - [q\gamma] < 2.$$

But $[p\beta] - [q\gamma]$ is a nonzero integer, hence it can only be either -1 or 1. In both cases $[p\beta]$ and $[q\gamma]$ are consecutive integers from $B \cup C$, which we have previously seen that is not possible. The contradiction thus obtained shows that our initial assumption is false, hence A, B, and C do not partition the set of positive integers, as stated.

This is problem B-6 from the 56th William Lowell Putnam Mathematical Competition, held in 1995.

11. We are given either that there exist integers p and q such that $f(p) = q^2$, and $f(p+1) = (q+1)^2$, or that there exist integers p and r such that $f(p) = (r+1)^2$, and $f(p+1) = r^2$. Nevertheless, the second case is basically the same as the first one, since then we also have $f(p) = q^2$, and $f(p+1) = (q+1)^2$ for $q = -r-1$. So, we place ourselves in the first case, when we know that

$$p^2 + ap + b = q^2$$

and

$$(p+1)^2 + a(p+1) + b = (q+1)^2.$$

By subtracting the first equation from the second, we get

$$2p + a = 2q,$$

which, by replacing $a = 2(q-p)$ in the first equation, yields

$$b = (q-p)^2.$$

Thus, for any integer n, we have that

$$f(n) = n^2 + 2(q-p)n + (q-p)^2 = (n+q-p)^2$$

is a square.

Alternatively, let $d = q - p$; hence we have

$$f(p) = (p+d)^2, \text{ and } f(p+1) = (p+1+d)^2.$$

Let g be defined by $g(x) = f(x) - (x+d)^2$. We have $g(p) = g(p+1) = 0$, and g is a polynomial function of degree (at most) one, therefore it must be identically zero, and $f(x) = (x+d)^2$ follows again.

12. There must exist nonzero real numbers a, b, and c, and real numbers u, v, and w such that

$$f(x)-g(x) = a(x-u)^2, \quad g(x)-h(x) = b(x-v)^2, \quad h(x)-f(x) = c(x-w)^2.$$

It follows

$$a(x-u)^2 + b(x-v)^2 + c(x-w)^2 = 0$$

for every real number x. Now by the pigeonhole principle, two of the numbers a, b, and c must have the same sign, so we can assume, without loss of generality, that these are a and b. The above equality for $x = w$ becomes

$$a(w-u)^2 + b(w-v)^2 = 0,$$

and it implies $w - u = w - v = 0$, hence $u = v = w$, as desired.

An example of such functions is

$$f(x) = 2x^2 + 2x + 4, \quad g(x) = x^2 + 4x + 3, \quad \text{and } h(x) = 4x^2 - 2x + 6$$

(and many other such examples can be found).

13. Let x_1 and x_2 be the zeros of f and let x_3 and x_4 be the zeros of g, so that we have $f(x) = (x-x_1)(x-x_2)$, $g(x) = (x-x_3)(x-x_4)$, $x_1 + x_2 = -a$, $x_1x_2 = b$, $x_3 + x_4 = -c$, and $x_3x_4 = d$. (In general x_1, x_2, x_3, and x_4 are complex numbers — possibly not real numbers.) We calculate

$$\begin{aligned} g(x_1)g(x_2) &= (x_1^2 + cx_1 + d)(x_2^2 + cx_2 + d) \\ &= (x_1x_2)^2 + c^2x_1x_2 + d^2 + cx_1x_2(x_1 + x_2) \\ &+ cd(x_1 + x_2) + d(x_1^2 + x_2^2) \\ &= b^2 + bc^2 + d^2 - abc - acd + d(a^2 - 2b) \\ &= (b-d)^2 + (a-c)(ad - bc) = R. \end{aligned}$$

Yet,

$$\begin{aligned} g(x_1)g(x_2) &= (x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4) \\ &= (x_3 - x_1)(x_3 - x_2)(x_4 - x_1)(x_4 - x_2) \\ &= f(x_3)f(x_4). \end{aligned}$$

Thus we have

$$R = f(x_3)f(x_4) = g(x_1)g(x_2) = (x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4).$$

Now we solve the problem. Suppose first that $R < 0$. This means, according to the above expressions of R, that

$$f(x_3)f(x_4) < 0 \text{ and } g(x_1)g(x_2) < 0.$$

Since f is a real quadratic function, and it has values of opposite signs for two real numbers (x_3 and x_4), it must have a real zero between x_3 and x_4, and then the other zero has to be real, too. Similarly, g has real roots. If we assume $x_1 < x_2$ and $x_3 < x_4$, we see immediately that

$$(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4) = R < 0$$

only holds if either $x_1 < x_3 < x_2 < x_4$, or $x_3 < x_1 < x_4 < x_2$, that is, for separated roots of f and g. Conversely, if the roots of f and g are real and separated one sees from this expression of R, that $R < 0$ follows, too.

Use this characterization of friendship for quadratic equations to give another solution to problem 2 from the chapter *Quadratic Functions and Quadratic Equations*!

Note that R is called the *resultant* of f and g and that, because of

$$R = (x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4),$$

we have $R = 0$ precisely when the equations $f(x) = 0$ and $g(x) = 0$ have a common root.

14. a) It is well-known that an orthonormal system (or basis) of vectors $\vec{i}$, $\vec{j}$, and $\vec{k}$ can be chosen in space such that any vector is expressible as a linear combination of $\vec{i}$, $\vec{j}$, and $\vec{k}$. These vectors $\vec{i}$, $\vec{j}$, and $\vec{k}$ are unit vectors (that is each one's length is 1), and are perpendicular to each other. Then any vector $\vec{s}$ in space can be uniquely expressed as

$$\vec{s} = x\vec{i} + y\vec{j} + z\vec{k},$$

for some real numbers x, y, and z. By using $\vec{i} \cdot \vec{j} = \vec{i} \cdot \vec{k} = \vec{j} \cdot \vec{k} = \vec{0}$ and $\vec{i}^2 = \vec{j}^2 = \vec{k}^2 = 1$ we immediately see that for

$$\vec{s}_1 = x_1\vec{i} + y_1\vec{j} + z_1\vec{k} \text{ and } \vec{s}_2 = x_2\vec{i} + y_2\vec{j} + z_2\vec{k}$$

we have

$$\vec{s}_1 \cdot \vec{s}_2 = x_1x_2 + y_1y_2 + z_1z_2.$$

In particular, for $\vec{s} = x\,\vec{i} + y\,\vec{j} + z\,\vec{k}$ we have

$$|\vec{s}|^2 = \vec{s}^{\,2} = \vec{s} \cdot \vec{s} = x^2 + y^2 + z^2,$$

and $\vec{s} \cdot \vec{i} = x$, $\vec{s} \cdot \vec{j} = y$, $\vec{s} \cdot \vec{k} = z$. Thus, we have $\vec{s} = \vec{0}$ if and only if the scalar product of $\vec{s}$ with each vector of the basis is zero.

So, for our problem, we will prove that the scalar product of any unit vector $\vec{v}$ with the sum $\vec{w}$ of all the given vectors (perpendicular to the faces of P) is 0, and, by the above observation, it will follow that $\vec{w} = \vec{0}$, as desired. We thus consider an arbitrary unit vector $\vec{v}$, and let π be a plane perpendicular to $\vec{v}$.

Let F be any face of P, and let $\vec{u}$ be the vector perpendicular to F, having the length equal to A, the area of F. Let α be the measure of the acute angle between the directions of $\vec{u}$ and $\vec{v}$, and observe that the acute angle between the plane of F and π also has measure α. Here by "acute' we mean with measure at most 90° (thus, actually, acute or right). This shows that the area of the projection of F on π equals the absolute value of the scalar product $\vec{u} \cdot \vec{v}$, namely $A\cos\alpha$.

The scalar product has, however, a sign. Assume that $\vec{v}$ is vertical and directed upwards, thus the plane π is horizontal. We split the faces of P into two families that we call upper faces and lower faces. An upper face F has the property that the scalar product of the corresponding vector $\vec{u}$ (perpendicular to F) with $\vec{v}$ is nonnegative (or, in other words, the projection of $\vec{u}$ on $\vec{v}$ is either directed upwards, as $\vec{v}$, or is null), while the lower faces are those for which that scalar product is negative. It is not hard to see that the sum of the areas of the projections on π of the upper faces equals the sum of the areas of the projections on π of lower faces, both being equal to the area of the projection of the polyhedron on π. Now, the sum of the scalar products of the form $\vec{u} \cdot \vec{v}$ (for all possible vectors $\vec{u}$) results to be $\vec{0}$, because it is the sum of the areas of the projections of the upper faces minus the sum of the areas of the projections of lower faces. This sum is precisely $\vec{w} \cdot \vec{v}$, and, since it is 0 for every unit vector $\vec{v}$, $\vec{w} = \vec{0}$ follows, as we intended to prove.

b) We know that if positive real numbers a, b, c, and d are given such that

$$a < b + c + d,\ b < a + c + d,\ c < a + b + d, \text{ and } d < a + b + c,$$

then a (planar) quadrilateral $ABCD$ exists such that the lengths of its sides are $a = AB$, $b = BC$, $c = CD$, and $d = DA$. (Prove it!)

We bend this quadrilateral along the diagonal AC in order to obtain a skew quadrilateral $ABCD$, still having the lengths of its sides $a = AB$, $b = BC$, $c = CD$, and $d = DA$. Denote by $\overrightarrow{a} = \overrightarrow{AB}$, $\overrightarrow{b} = \overrightarrow{BC}$, $\overrightarrow{c} = \overrightarrow{CD}$, and $\overrightarrow{d} = \overrightarrow{DA}$, so that the vectors $\overrightarrow{a}$, $\overrightarrow{b}$, $\overrightarrow{c}$, and $\overrightarrow{d}$ have lengths a, b, c, d respectively, and their sum

$$\overrightarrow{a} + \overrightarrow{b} + \overrightarrow{c} + \overrightarrow{d} = \overrightarrow{0}.$$

Moreover, any three of them are not coplanar.

Now consider four arbitrary planes, each of them orthogonal to one of the vectors $\overrightarrow{a}$, $\overrightarrow{b}$, $\overrightarrow{c}$, and $\overrightarrow{d}$. The planes intersect and form a tetrahedron. We denote by K_a, K_b, K_c, and K_d the areas of the faces of this tetrahedron (K_a being the area of the face perpendicular on $\overrightarrow{a}$, and so on). Next, we build a vector perpendicular to each face of the tetrahedron, directed towards the exterior of the tetrahedron, and having length equal to the area of that face. Let $\overrightarrow{K_a}$ be the vector perpendicular to the face of area K_a, and similarly define vectors $\overrightarrow{K_b}$, $\overrightarrow{K_c}$, and $\overrightarrow{K_d}$. The length of $\overrightarrow{K_a}$ is thus K_a, and so on.

By hedgehog's lemma we have

$$\overrightarrow{K_a} + \overrightarrow{K_b} + \overrightarrow{K_c} + \overrightarrow{K_d} = \overrightarrow{0}.$$

The vectors $\overrightarrow{d}$ and $\overrightarrow{K_d}$ are both perpendicular to the face of the tetrahedron of area K_d, thus there exists a real number p such that $\overrightarrow{K_d} = p\,\overrightarrow{d}$. Multiply the equality $\overrightarrow{a} + \overrightarrow{b} + \overrightarrow{c} + \overrightarrow{d} = \overrightarrow{0}$ by p and subtract from the above equality in order to get

$$\overrightarrow{K_a} - p\overrightarrow{a} + \overrightarrow{K_b} - p\,\overrightarrow{b} + \overrightarrow{K_c} - p\overrightarrow{c} = \overrightarrow{0}.$$

But vectors $\overrightarrow{K_a}$ and $\overrightarrow{a}$ are also orthogonal to the same plane, so there must be a real number α such that $\overrightarrow{K_a} = \alpha\overrightarrow{a}$, and, analogously, there exist real numbers β, and γ such that $\overrightarrow{K_b} = \beta\,\overrightarrow{b}$, and $\overrightarrow{K_c} = \gamma\overrightarrow{c}$. Thus, the previous equality becomes

$$(\alpha - p)\overrightarrow{a} + (\beta - p)\overrightarrow{b} + (\gamma - p)\overrightarrow{c} = \overrightarrow{0}.$$

However, the vectors $\overrightarrow{a}$, $\overrightarrow{b}$, and $\overrightarrow{c}$ are linearly independent (they are not in the same plane), hence the above equality yields all coefficients zero, that is

$$\alpha = \beta = \gamma = p.$$

By the very definition of p, we have that its absolute value $|p|$ is the ratio between the length of $\overrightarrow{K}_d$ and the length of $\overrightarrow{d}$, that is $|p| = K_d/d$.

Similarly $|\alpha| = K_a/a$, $|\beta| = K_b/b$, and $|\gamma| = K_c/c$.
Thus $|\alpha| = |\beta| = |\gamma| = |p|$ actually means that

$$\frac{K_a}{a} = \frac{K_b}{b} = \frac{K_c}{c} = \frac{K_d}{d}.$$

In other words, the areas of the faces of the tetrahedron that we built are proportional to the given numbers a, b, c, and d. Clearly a well-suited similarity transforms this tetrahedron into another one whose areas of faces are precisely the numbers a, b, c, and d, and our proof finishes here.

15. This is the same as problem 16 from the chapter *The Scalar Product*, but we come here with another solution (still based on the properties of the scalar product). We will need in our proof the theorem of three perpendiculars; since this result might be less known, we remind it first. The theorem of three perpendiculars states that, given a plane π a straight line XY perpendicular to π, with $Y \in \pi$, a straight line $l \subset \pi$, and the (orthogonal) projection Z of Y on l, XZ is also perpendicular on l. The converse is also true, in the sense that if we consider Z to be the projection of X on l (the rest of the hypothesis remaining valid), then $YZ \perp l$ follows, too.

    We also intend to use hedgehog's lemma (from the previous problem) again, thus we start by considering vectors $\overrightarrow{v_1}$, $\overrightarrow{v_2}$, $\overrightarrow{v_3}$, and $\overrightarrow{v_4}$ perpendicular to the faces opposite to A_1, A_2, A_3, and A_4 respectively, directed towards the exterior of the tetrahedron, and having lengths K_1, K_2, K_3, and K_4 respectively. We have, according to the mentioned result,

    $$\overrightarrow{v_1} + \overrightarrow{v_2} + \overrightarrow{v_3} + \overrightarrow{v_4} = \overrightarrow{0}.$$

    We express vectors $\overrightarrow{v_s}$ in coordinates, as

    $$\overrightarrow{v_s} = x_s \overrightarrow{i} + y_s \overrightarrow{j} + z_s \overrightarrow{k}$$

    with real numbers x_s, y_s, and z_s, for $s = 1, 2, 3, 4$. As in the solution of the previous problem, $\overrightarrow{i}$, $\overrightarrow{j}$, and $\overrightarrow{k}$ form an orthonormal basis for the vectors from space, that is, $\overrightarrow{i}$, $\overrightarrow{j}$, and $\overrightarrow{k}$ are unit vectors orthogonal to each other. The properties of $\overrightarrow{v_s}$, $s = 1, 2, 3, 4$ expressed in terms of coordinates are

    $$x_1^2 + y_1^2 + z_1^2 = (K_1^2 = K_2^2 =) x_2^2 + y_2^2 + z_2^2,$$
    $$x_3^2 + y_3^2 + z_3^2 = (K_3^2 = K_4^2 =) x_4^2 + y_4^2 + z_4^2,$$

    and

    $$x_1 + x_2 + x_3 + x_4 = y_1 + y_2 + y_3 + y_4 = z_1 + z_2 + z_3 + z_4 = 0.$$

We square $x_1+x_3=-x_2-x_4$, $y_1+y_3=-y_2-y_4$, and $z_1+z_3=-z_2-z_4$ in order to obtain

$$x_1^2+x_3^2+2x_1x_3=x_2^2+x_4^2+2x_2x_4,$$

$$y_1^2+y_3^2+2y_1y_3=y_2^2+y_4^2+2y_2y_4,$$

and

$$z_1^2+z_3^2+2z_1z_3=z_2^2+z_4^2+2z_2z_4.$$

By adding these equalities, and using

$$x_1^2+y_1^2+z_1^2=x_2^2+y_2^2+z_2^2 \quad \text{and} \quad x_3^2+y_3^2+z_3^2=x_4^2+y_4^2+z_4^2,$$

we get

$$x_1x_3+y_1y_3+z_1z_3=x_2x_4+y_2y_4+z_2z_4$$

that is, $\overrightarrow{v_1}\cdot\overrightarrow{v_3}=\overrightarrow{v_2}\cdot\overrightarrow{v_4}$. By the definition of the scalar product, this, on its turn, means

$$K_1K_3\cos\angle(\overrightarrow{v_1},\overrightarrow{v_3})=K_2K_4\cos\angle(\overrightarrow{v_2},\overrightarrow{v_4}).$$

Because $K_1=K_2$ and $K_3=K_4$, this means that the angles formed by $\overrightarrow{v_1}$ with $\overrightarrow{v_3}$ and by $\overrightarrow{v_2}$ with $\overrightarrow{v_4}$ are equal.

But we can construct these angles in the following way, too.
Let $A_1H_1\perp(A_2A_3A_4)$, with $H_1\in(A_2A_3A_4)$ (here and further (XYZ) is the plane determined by the non-collinear points X, Y, and Z). Then let $H_1M_1\perp A_2A_4$, with $M_1\in A_2A_4$. By the theorem of three perpendiculars, we also have $A_1M_1\perp A_2A_4$, hence $\angle A_1M_1H_1$ is the angle between the planes $(A_1A_2A_4)$ and $(A_2A_3A_4)$, having thus the same measure as the angle of vectors $\overrightarrow{v_1}$ and $\overrightarrow{v_3}$. Similarly, if we build $A_2H_2\perp(A_1A_3A_4)$, with $H_2\in(A_1A_3A_4)$, and $H_2M_2\perp A_1A_3$, with $M_2\in A_1A_3$, the angle $\angle A_2M_2H_2$ has the same measure as the angle of vectors $\overrightarrow{v_2}$ and $\overrightarrow{v_4}$. Consequently, the angles $\angle A_1M_1H_1$ and $\angle A_2M_2H_2$ have equal measures.

On the other hand, A_1H_1 and A_2H_2 are heights of the tetrahedron corresponding to its faces $A_2A_3A_4$ and $A_1A_3A_4$ of equal areas, therefore (by expressing the volume of the tetrahedron in two ways) $A_1H_1=A_2H_2$ follows. Consequently, the right triangles $A_1H_1M_1$ and $A_2H_2M_2$ are congruent, thus we also have $A_1M_1=A_2M_2$. But the areas of $A_1A_2A_3$ and $A_1A_2A_4$ are equal, hence

$$\frac{A_1M_1\cdot A_2A_4}{2}=\frac{A_2M_2\cdot A_1A_3}{2},$$

yielding $A_2A_4=A_1A_3$.

We are sure that the reader will now be able to prove analogously the other required equality, $A_1A_4 = A_2A_3$, by first showing that $\overrightarrow{v_1} \cdot \overrightarrow{v_4} = \overrightarrow{v_2} \cdot \overrightarrow{v_3}$, then following precisely the same approach as above. The proof ends here.

16. Let $\omega = \cos(2\pi/3) + i\sin(2\pi/3)$. We can consider that the vertices of the triangles have the affixes $A_1(a)$, $B_1(a\omega)$, $C_1(a\omega^2)$, and $A_2(b)$, $B_2(b\omega)$, $C_2(b\omega^2)$, for some complex numbers a and b (by taking the common center of the triangles to be the origin of the complex plane). Because the triangles do not coincide, b is different from any of a, $a\omega$, and $a\omega^2$. Let $M(z)$ be the point of intersection of the lines B_1C_2 and B_2C_1. Thus we have

$$z = (1-\alpha)a\omega + \alpha b\omega^2 \Leftrightarrow \alpha = \frac{z - a\omega}{b\omega^2 - a\omega}$$

and

$$z = (1-\beta)a\omega^2 + \beta b\omega \Leftrightarrow \beta = \frac{z - a\omega^2}{b\omega - a\omega^2}$$

for real numbers α and β. Now consider the number

$$\gamma = \frac{z-a}{b-a}$$

and notice that the equalities

$$\alpha + \beta + \gamma = \alpha\beta + \alpha\gamma + \beta\gamma = \frac{3abz - 3a^3}{b^3 - a^3}$$

hold, due to the relations $\omega^3 = 1$ and $\omega^2 + \omega + 1 = 0$ satisfied by ω; thus

$$\gamma(1 - \alpha - \beta) = \alpha\beta - \alpha - \beta.$$

If we had $1 - \alpha - \beta = 0$, then $\alpha\beta - \alpha - \beta = 0$ would also follow, hence we would get $\alpha + \beta = \alpha\beta = 1$, which would lead to non-real values for α and β. Thus, we have $1 - \alpha - \beta \neq 0$, and

$$\gamma = \frac{\alpha\beta - \alpha - \beta}{1 - \alpha - \beta}$$

follows, which shows that γ is also a real number. Finally,

$$z = (1-\gamma)a + \gamma b$$

with real γ means that $M(z)$ is a point on the line through $A_1(a)$, and $A_2(b)$, therefore the lines A_1A_2, B_1C_2, and B_2C_1 concur at M.

17. The limits of the three sequences are all equal to 1/3. Let M be the matrix

$$M = \begin{pmatrix} p & r & q \\ q & p & r \\ r & q & p \end{pmatrix}.$$

From the recurrence relations we infer that

$$\begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} = \begin{pmatrix} p & r & q \\ q & p & r \\ r & q & p \end{pmatrix} \begin{pmatrix} x_{n-1} \\ y_{n-1} \\ z_{n-1} \end{pmatrix} = M \begin{pmatrix} x_{n-1} \\ y_{n-1} \\ z_{n-1} \end{pmatrix},$$

for every $n \geq 1$. Then, by an easy induction, we have

$$\begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} = \begin{pmatrix} p & r & q \\ q & p & r \\ r & q & p \end{pmatrix}^n \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = M^n \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix},$$

and

$$M^n = \begin{pmatrix} x_n & z_n & y_n \\ y_n & x_n & z_n \\ z_n & y_n & x_n \end{pmatrix},$$

for any $n \geq 0$. There is a not so big difference between the case of second order matrices and linear recurrences of second order (which we have studied in a previous chapter), and the case of third order matrices and linear recurrences of third order. Namely, because M satisfies its characteristic equation

$$M^3 - 3pM^2 + 3(p^2 - rq)M - (p^2 + q^2 + r^2 - pq - pr - qr)I_3 = O_3$$

we have that

$$M^n - 3pM^{n-1} + 3(p^2 - rq)M^{n-2} - (p^2 + q^2 + r^2 - pq - pr - qr)M^{n-3} = O_3,$$

and, consequently,

$$x_n - 3px_{n-1} + 3(p^2 - rq)x_{n-2} - (p^2 + q^2 + r^2 - pq - pr - qr)x_{n-3} = 0$$

for all $n \geq 3$. Yet, the sequences $(y_n)_{n\geq 0}$ and $(z_n)_{n\geq 0}$ verify the same recurrence relation.

The characteristic equation of this recurrence (as the characteristic equation of the matrix M) is

$$t^3 - 3pt^2 + 3(p^2 - qr)t - (p^2 + q^2 + r^2 - pq - pr - qr) = 0.$$

(A parenthesis is, maybe, necessary. The characteristic equation of a third order matrix A is $t^3 - \operatorname{Tr}(A)t^2 + S(A)t - \det(A)I_3 = O_3$, where $\operatorname{Tr}(A)$ is the trace of the matrix — the sum of the elements on its main diagonal — $S(A)$ is the sum of its second order diagonal co-factors, and $\det(A)$ is the determinant of the matrix. In our case,

$$\begin{aligned}\det(A) &= p^3 + q^3 + r^3 - 3pqr = (p+q+r)(p^2+q^2+r^2-pq-pr-qr)\\ &= p^2+q^2+r^2-pq-pr-qr\end{aligned}$$

because $p+q+r=1$ is given.)

The characteristic equation can also be written as

$$(t-1)(t^2+(1-3p)t+p^2+q^2+r^2-pq-pr-qr)=0$$

(use $p+q+r=1$ again in order to check this). Thus its zeros are t_1, t_2, and 1, where t_1 and t_2 are the zeros of the quadratic equation

$$t^2+(1-3p)t+p^2+q^2+r^2-pq-pr-qr=0,$$

whose discriminant is

$$\begin{aligned}\Delta &= (1-3p)^2 - 4(p^2+q^2+r^2-pq-pr-qr)\\ &= (q+r-2p)^2 - 4(p^2+q^2+r^2-pq-pr-qr)\\ &= -3(q-r)^2 \le 0.\end{aligned}$$

If $\Delta < 0$ (when $q \neq r$), t_1 and t_2 are complex conjugate (not real) numbers whose product is

$$p^2+q^2+r^2-pq-pr-qr < (p+q+r)^2 = 1.$$

If $q=r$, $t_1 = t_2 \in \mathbb{R}$ follows and their product is again less than 1. In both cases, we get $|t_1| = |t_2| < 1$. The general term of the sequence $(x_n)_{n\geq 0}$ will be either of the form

$$x_n = A + Bt_1^n + Ct_2^n,$$

(when t_1 and t_2 are complex conjugates), or of the form

$$x_n = A + (B+nC)t_1^n$$

(when $t_1 = t_2$), for some numbers A, B, C (and the same is true for y_n and z_n). Anyway, because t_1 and t_2 have absolute values less than 1, the convergence of $(x_n)_{n\geq 0}$ follows (and, analogously, we get that $(y_n)_{n\geq 0}$ and $(z_n)_{n\geq 0}$ are convergent).

If we denote by x, y, and z the limits of $(x_n)_{n\geq 0}$, $(y_n)_{n\geq 0}$, and $(z_n)_{n\geq 0}$ respectively, by passing to the limit in the recurrence relations, we get

$$\begin{aligned} x &= px + ry + qz \\ y &= qx + py + rz \\ z &= rx + qy + pz. \end{aligned}$$

This system of linear equations has the general solution $x = y = z$.

On the other hand, by adding side by side the recurrence relations, we obtain

$$x_n + y_n + z_n = (p + q + r)(x_{n-1} + y_{n-1} + z_{n-1}) = x_{n-1} + y_{n-1} + z_{n-1}$$

for all $n \geq 1$, which leads to

$$x_n + y_n + z_n = x_0 + y_0 + z_0 = 1$$

for all $n \geq 0$. Passing to the limit in this equation for $n \to \infty$ we get $x + y + z = 1$, thus, finally, $x = y = z = 1/3$.

Bibliography

1. Martin Aigner, Günter M. Ziegler, *Proofs from THE BOOK*, Springer, 2003.
2. Horea Banea, *Probleme de matematică traduse din revista sovietică "Kvant"*, Editura Didactică şi Pedagogică, Bucureşti, 1983.
3. Béla Bollobás, *The Art of Mathematics – Coffee Time in Memphis*, Cambridge University Press, 2006.
4. Constantin Cocea, *200 de probleme din geometria triunghiului echilateral*, Editura Gh. Asachi, Iaşi, 1992.
5. Arthur Engel, *Problem-Solving Strategies*, Problem Books in Mathematics, Springer, 1998.
6. G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, 4th edition, Oxford University Press, 1960.
7. G.H. Hardy, J.E. Littlewood, G. Pòlya, *Inequalities*, Cambridge University Press, 1934.
8. I.N. Herstein, *Topics in Algebra*, Xerox College Publishing, 2nd edition, 1975.
9. A.I. Kostrikin, *Introduction à l'algèbre*, Mir, 1981.
10. Serge Lang, *Algebra*, 3rd edition, Undergraduate Texts in Mathematics, Springer, 2002.
11. Laurenţiu Panaitopol, Alexandru Gica, *Probleme de aritmetică şi teoria numerelor. Idei şi metode de rezolvare*, Editura Gil, 2006.
12. V.V. Prasolov, *Essays on Numbers and Figures*, Mathematical World, American Mathematical Society, 2000.
13. Walter Rudin, *Principles of Mathematical Analysis*, McGraw-Hill, Inc., 1976.
14. W. Sierpinski, *Elementary Theory of Numbers*, North-Holland Mathematical Library, PWN-Polish Scientific Publishers, 1988.

Other Books from XYZ Press

1. Matei, V., Reiland, E., *112 Combinatorial Problems from the AwesomeMath Summer Program*, 2016.
2. Andreescu, A., Vale, V., *111 Problems in Algebra and Number Theory*, 2016.
3. Andreescu, T., *Mathematical Reflections - two special years*, 2016.
4. Andreescu, T., Pohoata, C., Korsky, S., *Lemmas in Olympiad Geometry*, 2016.
5. Mihalescu, C., *The Geometry of Remarkable Elements. Points, lines, and circles*, 2016.
6. Andreescu, T., Pohoata, C., *110 Geometry Problems for the International Mathematical Olympiad*, 2015.
7. Andreescu, T., Boreico, I., Mushkarov, O., Nikolov, N., *Topics in Functional Equations*, 2nd edition, 2015.
8. Andreescu, T., Ganesh, A., *109 Inequalities from the AwesomeMath Summer Program*, 2015.
9. Andreescu, T., Pohoata, C., *Mathematical Reflections - two great years*, 2014.
10. Andreescu, T., Ganesh, A., *108 Algebra Problems from the AwesomeMath Year-Round Program*, 2014.
11. Andreescu, T., Kisačanin, B., *Math Leads for Mathletes – a rich resource for young math enthusiasts, parents, teachers, and mentors*, Book 1, 2014.
12. Becheanu, M., Enescu, B., *Balkan Mathematical Olympiads – the first 30 years*, 2014.
13. Andreescu, T., *Mathematical Reflections – two more years,* 2013.
14. Andreescu, T., Rolinek, M., Tkadlec, J., *107 Geometry Problems from the AwesomeMath Year-Round Program*, 2013.

15. Andreescu, T., Rolinek, M., Tkadlec, J., *106 Geometry Problems from the AwesomeMath Summer Program*, 2013.
16. Andreescu, T., *105 Algebra Problems from the AwesomeMath Summer Program*, 2013.
17. Andreescu, T., Kane, J., *Purple Comet Math Meet! - the first ten years*, 2013.
18. Andreescu, T., *Mathematical Reflections - the next two years*, 2012.
19. Andreescu, T., Dospinescu, G., *Straight from the Book*, 2012.
20. Andreescu, T., *Mathematical Reflections – the first two years*, 2011.
21. Andreescu, T., Dospinescu, G., *Problems from the Book*, 2nd edition, 2010.

Coming soon

22. Bosch, R., *Cuban Mathematical Olympiads (2001-2016).*
23. Andreescu, T., Crisan, V., *Mathematical Induction. A powerful and elegant method of proof.*
24. Andreescu, A., Andreescu, T., Mushkarov, O., *113 Geometric Inequalities from the AwesomeMath Summer Program.*
25. Andreescu, T., Elliott, S., *114 Exponent and Logarithm Problems from the AwesomeMath Summer Program.*

Printed by "Combinatul Poligrafic"
Com. nr. 61610